Blue Crab Shells

Offensive Rust for Windows

Michael Taggart

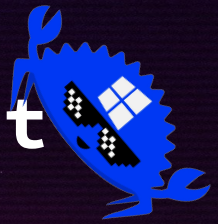
Who Am I?

- Senior Researcher
- Threat Hunting
- Adversarial Emulation
- Educator
- Streamer
- Collector of Rare Programming Languages

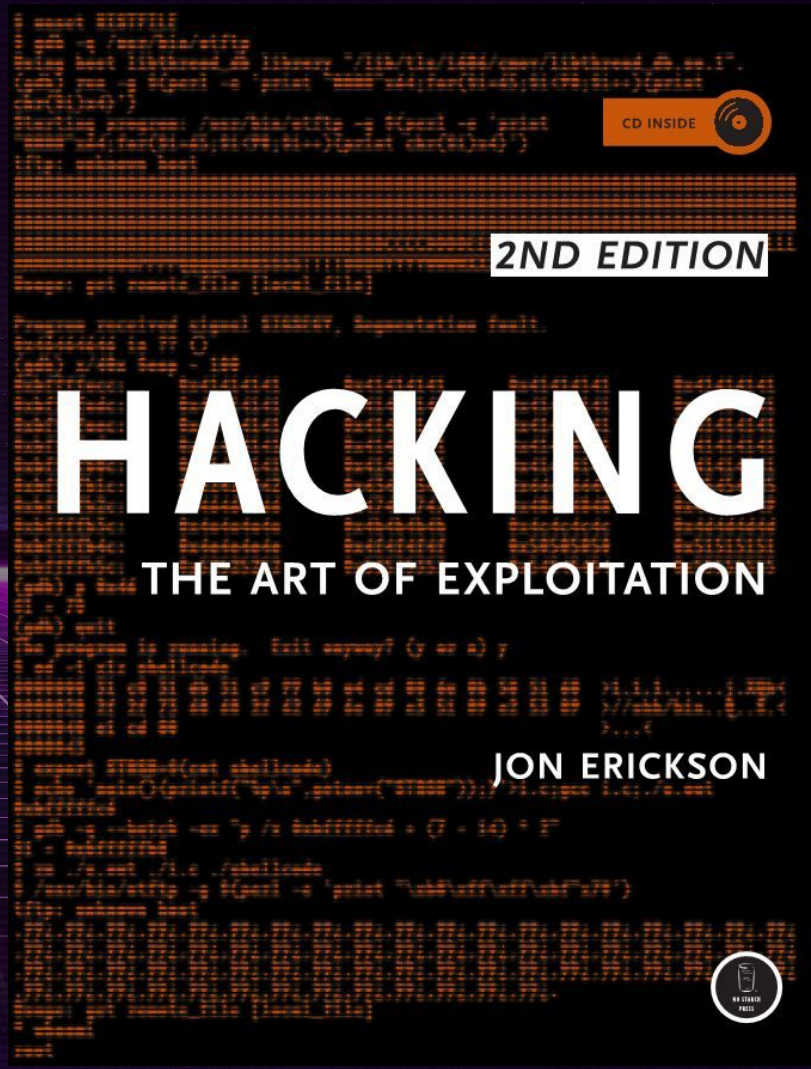

THE TAGGART INSTITUTE
MASTER YOUR CRAFT
taggartinstitute.org | discord.gg/taggartinstitute

Who Are You?

How I Got Into Rust



- Came from web dev
- Played with Rust in early days
- Totally whiffed on *Hacking: The Art of Exploitation*
- Missed C and went right to Rust



Getting Offensive

- OffensiveNotion
  - github.com/mttaggart/offensivenotion
- Notion as a C2
- Originally going to be in Nim
- Bugs in Nim sent us to Rust
  Never looked back

What You've Heard

- Rust is hard
- Systems language
- "Memory-safe" (OR IS IT???)
- Fast
- Huge Binaries

What's True

- Rust **syntax** is hard
- Memory model takes practice
- Great dev experience
- Lower-level power, higher-level ergonomics
- FFI
- Big binaries, but not as big as you think

What’s True for Offense

- Simple Cross-Compilation
- Conditional Compilation for multi-platform payloads
- Excellent Windows API Integration
- Disassemblers struggle with Rust
- Fast, and with concurrency? 👀

Today’s Objectives

- Set up Rust Dev Environment
- Build a Rudimentary C2
- Attack our target machine

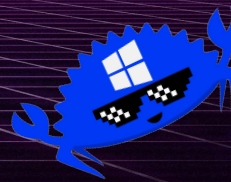
To Play Along, You'll Need:

- A laptop
- Ideal: Windows Subsystem for Linux
- Or: Linux with a Windows VM
- These slides (and code) will be available
- Code:
  https://github.com/The-Taggart-Institute/blue-crab-shells

github.com/The-Taggart-Institute/blue-crab-shells

Session Breakdown

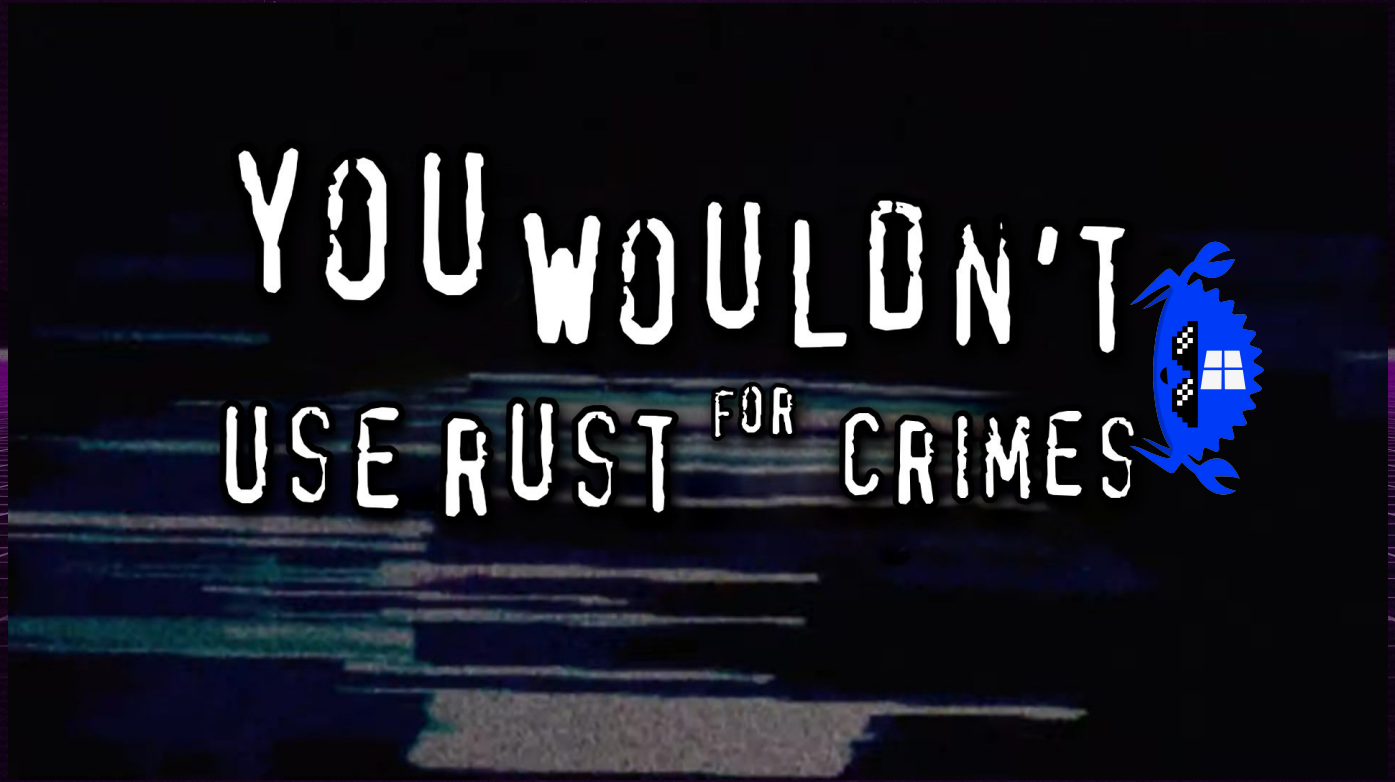
- Part 1: Getting our Crab Legs
  - Dev environment setup
  - Basic communication/execution
- Part 2: Rusting it Up A Notch
  - Windows API Review
  - Additional features
  - DLLs?!



Agreements

- I am not the world’s best programmer
- Some of the code is inelegant
  - Sometimes that’s me being me
  - Sometimes it’s for teaching purposes
- Questions should be for gaining knowledge, not proving knowledge

Agreements



Rust Dev Environment

Stage 0:
Hello, World!

Stage 1:
Hello, Windows!

Stage 2: Communication

Stage 3: Execution

Stage 4: C2Command

Stage 5:
Code Cleanup

Questions So Far

Stage 6: Persistence

Stage 7: Persistence

Stage 8: DLL Mode

Stage 9:
Final Form

Going Further

- *Black Hat Rust* by Sylvain Kerkour
- RustRedOps/Offensive Rust Repos
-

Thank You!
Questions?

mttaggart@infosec.town