VACCINATION

THE ANTI-HONEYPOT APPROACH
WHOAMI

• Researcher @ Minerva Labs, an Israeli startup
• Big fan of breaking stuff and putting them back together
• Expert in calling experts when failing to put stuff back together
• Fluent in C, C#, Python, Java and… Arabic
• Twitter: @Gal_B1t
WHAT IS A HONEYPOT?
THAT LADY IN RED

- Honeypots are that first girl to appear in a Bond movie
- From far away they look like a catch
- Up close it is clear they ain’t a bargain
SO....
WHAT IS A ANTI-HONEYPOT?
NATURAL APPROACH FOR REPELLING ATTACKERS

• Can you tell the difference?
EVEN BUTTERFLIES TRY TO FIND HACKS
KNOW YOUR ENEMY’S FEARS - FOUR WAYS TO REPEL BAD GUYS
VIRTUALIZED ANALYSIS ENVIRONMENT

- Goals:
  - Misleading the poor reverser directly
  - Fooling analysis tools
- Seeking after hints for the presence of:
  - Static and dynamic analysis tools
  - Virtualization or emulation infrastructure

```c
push NULL
push .szWindowClassOllyDbg
call [FindWindowA]
test eax,eax
jnz .debugger_found

push NULL
push .szWindowClassWinDbg
call [FindWindowA]
test eax,eax
jnz .debugger_found

.sｚWindowClassOllyDbg db "OLLYDBG",0
.sｚWindowClassWinDbg db "WinDbgFrameClass",0
```
HEAVILY FORTIFIED TARGETS

• Evading specific security products — the attacker’s advantage
• Can’t beat them all, but 90% of them is enough
• More in the live demo!
• Bugs in implementation of infection markers
• Abusing proper mechanisms
AND SPORA RANSOMWARE!

https://github.com/MinervaLabsResearch/SporaVaccination
• Be careful with what you wish for when vaccinating!

• Russian keyboard:
  • Some malware will avoid to infect you
  • Others are comrade-targeted malware
HOW BAD GUYS KNOW WHEN TO BUG OUT?
STATIC WINDOWS ARTIFACTS

• Registry keys
• Registry values
• Files
• Folders

Can be created persistently!
DYNAMIC WINDOWS ARTIFACTS

- Processes
- Mutexes
- Windows
- Requires different approach:
  - Run 1,000 programs, create 1,000 windows and 1,000 mutexes
  - More clever low level solutions are at hand

```python
def create_exe(name):
    dest_file = temp_folder + name
    shutil.copyfile(src_proc, dest_file)

def run_exe(command):
    try:
        subprocess.Popen(command)
    except Exception as e:
        print("Got exception \(\{0\}\) while creating \(\{1\}\).\).format(e, command)
    return

if __name__ == '__main__':
    processes_to_mimic = [
        "\Wireshark.exe",
        "\OLLYDBG.exe",
        "\vmtoolsd.exe",
        "\mspaint.exe"
    ]

    for proc_name in processes_to_mimic:
        create_exe(proc_name)
        run_exe(temp_folder + proc_name)

    while True:
        pass
```
LOW LEVEL X86 TRICKS

• “Red Pill” (Joanna Rutkowska, 11/2004)

```c
int swallow_redpill () {
    unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";
    *((unsigned*)&rpill[3]) = (unsigned)m;
    ((void(*)(void))&rpill)();
    return (m[5]>0xd0) ? 1 : 0; // return 1 if in VM.
}
```

• Why bother?
DEMO TIME!

https://github.com/G4LB1T/TC2017
QUESTIONS?