



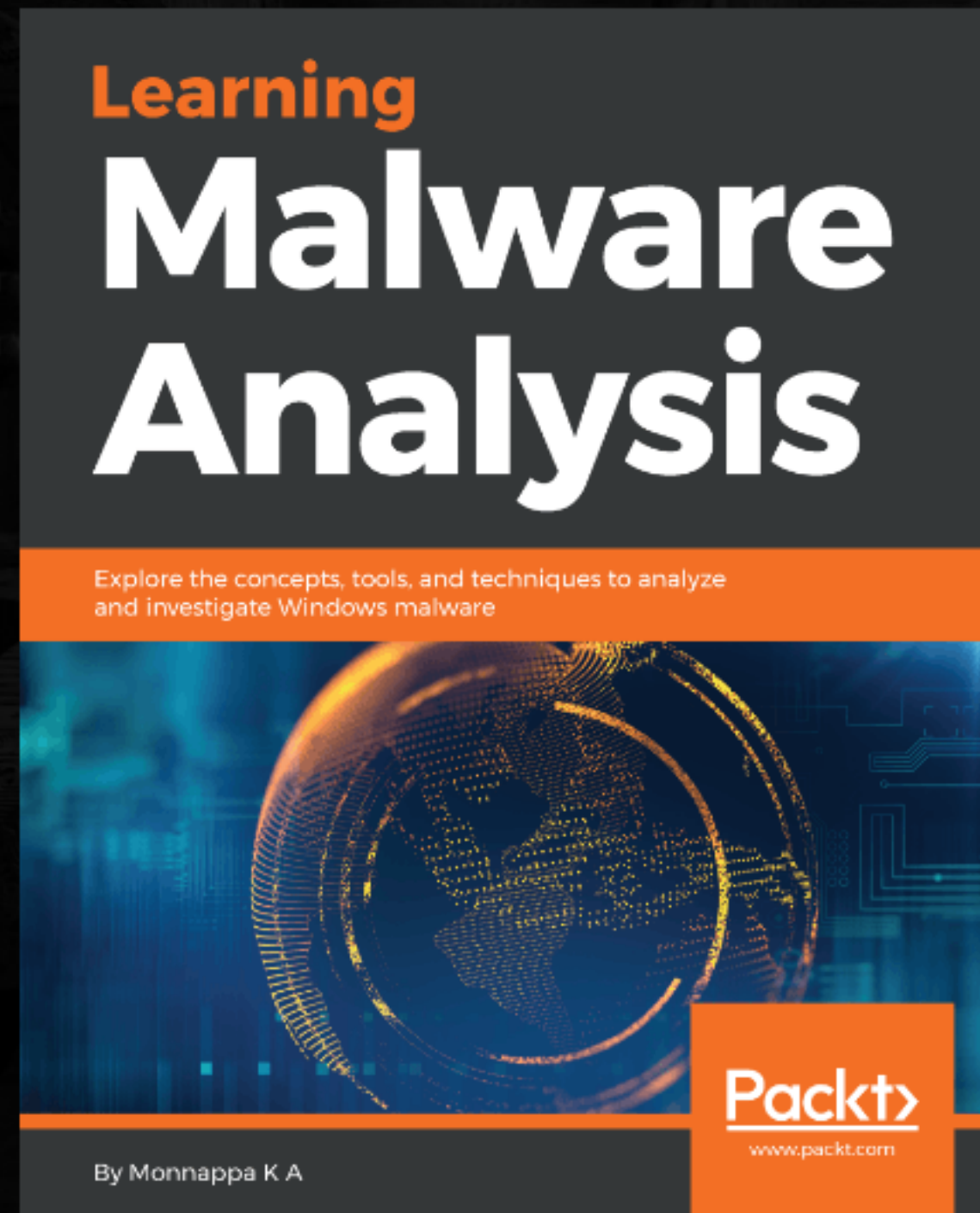
Hunting Gh0stRat in Memory

Gh0stRat Introduction

- **Gh0stRat** is a RAT (Remote Access Trojan)
- Used in many APT/targeted attacks like "**Gh0stnet**" against Private Office of the Dalai Lama
- Used to attack large corporations in the oil and gas industry dubbed as "**Operation Night Dragon**"
- When a host is infected with Gh0stRat, the malware collects the system information, encrypts the collected information and sends it to the C2 (command and control) server

Demo 9 - Hunting Gh0stRAT from Memory

Reference Book



THANK YOU



monnappa22@gmail.com



<https://cysinfo.com>



[@monnappa22](https://twitter.com/monnappa22)



<http://www.youtube.com/c/MonnappaKA>