Malware Unpacking Workshop

Lilly Chalupowski
August 28, 2019

whois lilly.chalupowski

Table: *who.is results*

Name	Lilly Chalupowski
Status	Employed
Creation Date	1986
Expiry	A Long Time from Now (Hopefully)
Registrant Name	GoSecure
Administrative Contact	Travis Barlow
Job	Threat Intelligence - Team Lead

Agenda

What will we cover?

- Disclaimer
- Reverse Engineering Concepts
  - Registers
  - Stack
  - Heap
  - Assembly
  - Calling Conventions
- Tools
  - x64dbg
  - Cutter
  - Radare2
- Malware Unpacking Concepts
- Exercise

Disclaimer

Don't be a Criminal

disclaimer.log

The tools and techniques covered in this presentation can be dangerous and are being shown for educational purposes.

It is a violation of Federal laws to attempt gaining unauthorized access to information, assets or systems belonging to others, or to exceed authorization on systems for which you have not been granted.

Only use these tools with/on systems you own or have written permission from the owner. I (the speaker) do not assume any responsibility and shall not be held liable for any illegal use of these tools.