CSC840 LAB 15
REVERSE ENGINEERING AN OBFUSCATED LINUX BEACON

PRESENTED BY: TAYLOR MARRION

WHY WE CARE

WHY OBFUSCATE MALWARE?

- Hide configuration and indicators
- Evade string-based detection
- Delay static analysis

WHY ANALYSTS MUST ADAPT

- Behavior still exists
- Configuration must be decoded at runtime
- Reverse engineering bridges the gap

THREE MAIN IDEAS

- Obfuscation removes indicators, not behavior
- Analysts hunt decode logic, not strings
- Plaintext must exist before use

SINGLE SOURCE, MULTIPLE ANALYSIS SURFACES

- Plaintext Beacon
  - Configuration stored as readable strings
- Encoded Beacon
  - Configuration stored as XOR-encoded byte arrays
- Encoded + Stripped Beacon
  - Same encoding, symbols removed *(time pending)*

DEMO

- Check this out! (click me for youtube link)

WHERE DO WE GO FROM HERE?

- Stronger Obfuscation
  - XOR → real cryptography
- Automation
  - Build extractor, script decoding
- Dynamic Analysis
  - Use debugger to capture decoded data at runtime
- Detection & Defense
  - Develop signatures based on decode-before-use behavior
  - Focus on behavioral indicators instead of static strings

HAPPY NEW YEAR!

Thanks for the wonderful semester!