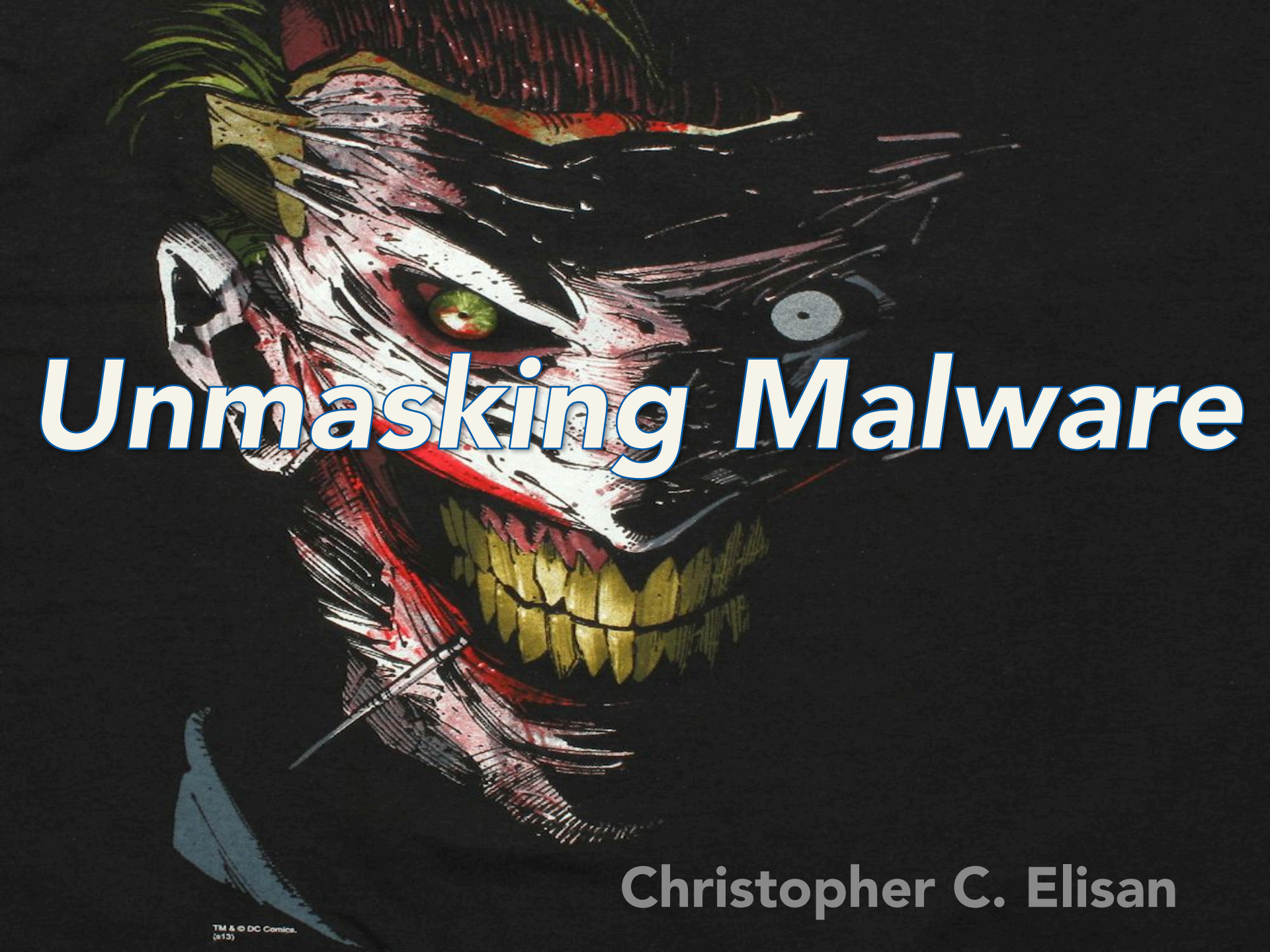

Unmasking Malware
Christopher C. Elisan
TM & © DC Comics.
(s13)

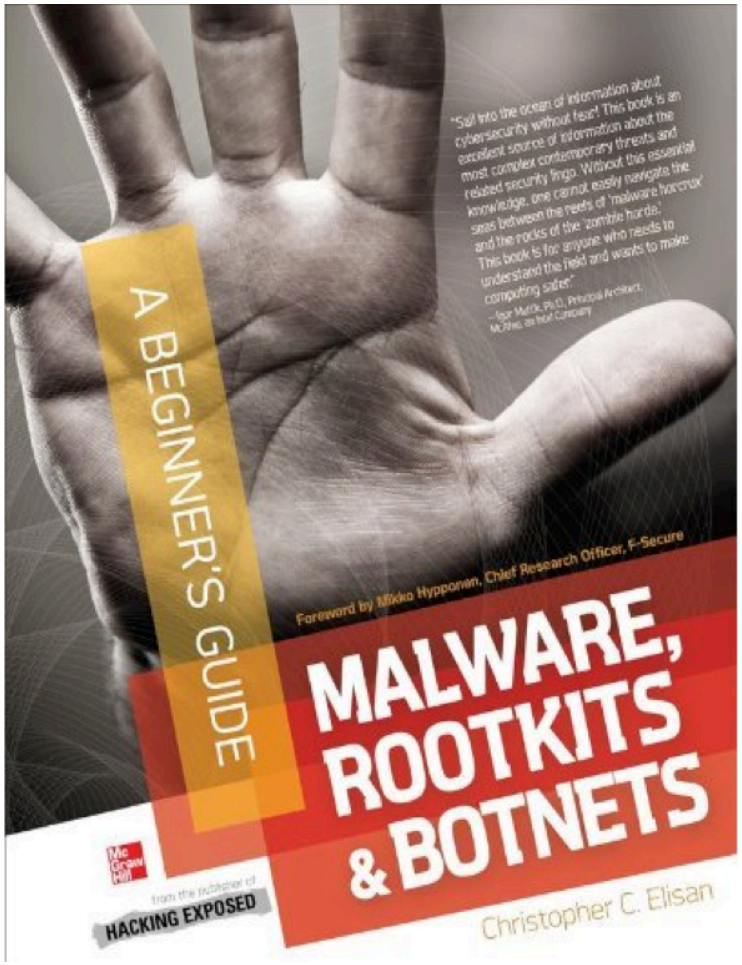
RSA FirstWatch

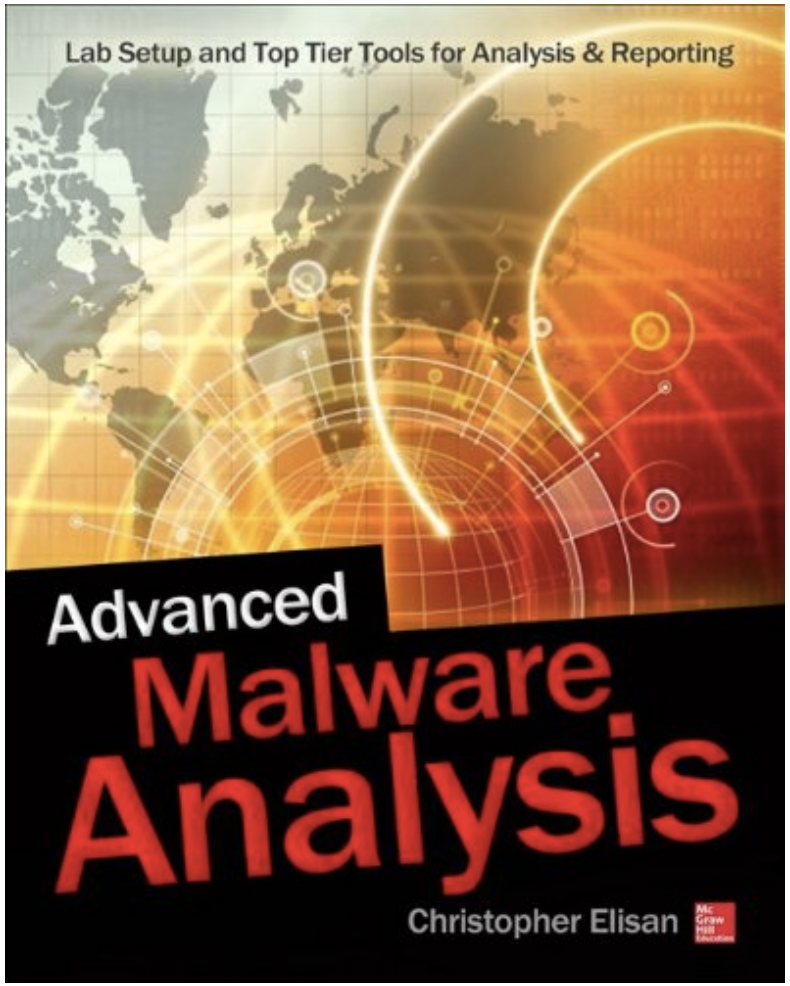
About Me

- Principal Malware Scientist / Sr. Manager MIT
- Past Adventures
  - Damballa
  - F-Secure
  - Trend Micro
- @Tophs

RSA FirstWatch

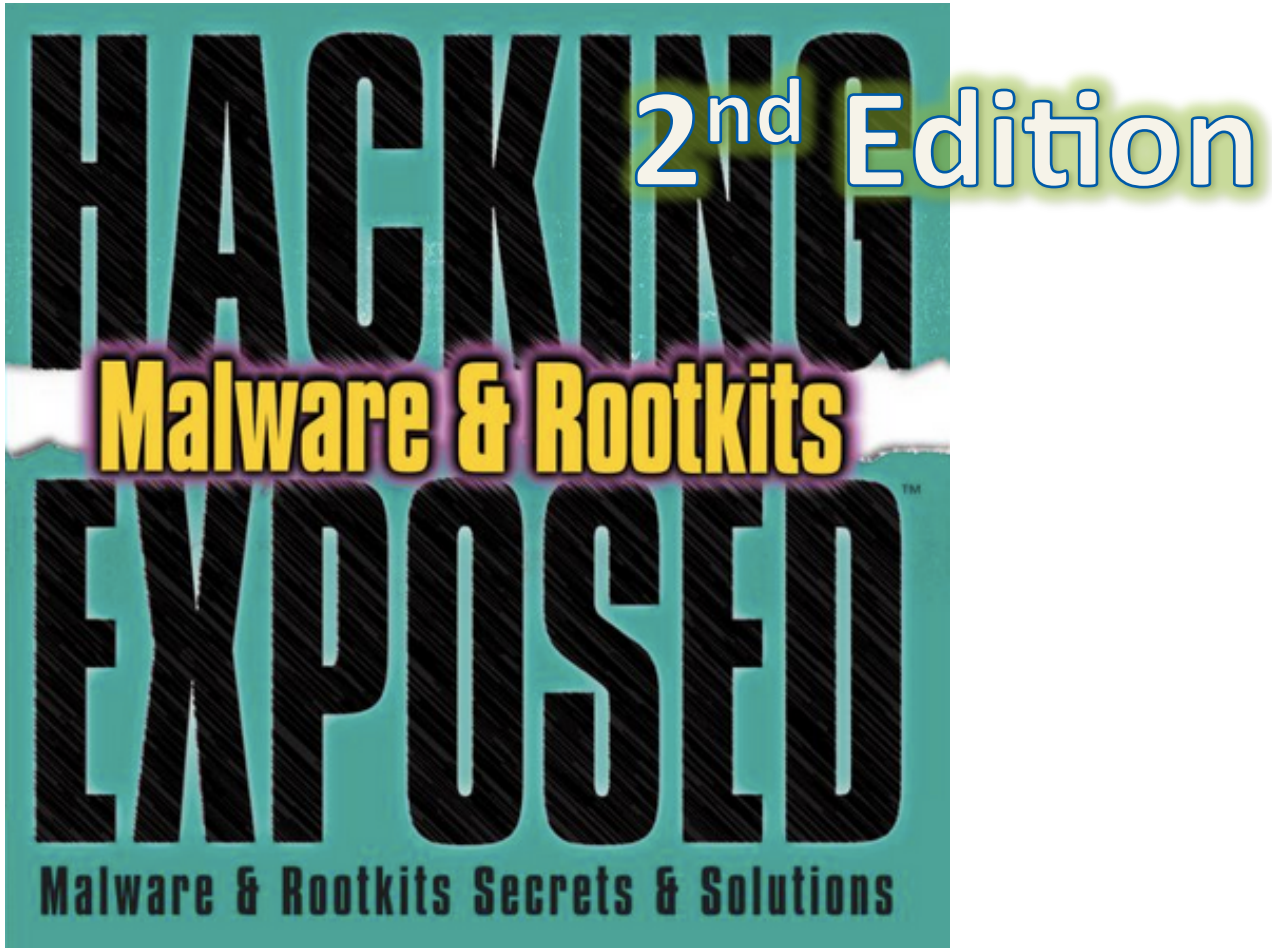
Author of





RSA FirstWatch

Co-Author of



2016

RSA
FirstWatch

Let the Fun Stuff Begins…

RSA FirstWatch

Agenda

- Different techniques to protect malware
- Automated malware masking
- Techniques on how to unmask malware

RSA FirstWatch

Malware Masking Techniques

- Code Obfuscation
- Basic Encryption
- Metamorphism
- Polymorphism
- Packing (Size Reduction and Encryption)

RSA FirstWatch

DEMO

Automated Malware Masking

RSA FirstWatch

Unmasking Malware Techniques

- **Freely available tools**
- **Debugging**
- **Memory Capture**

RSA FirstWatch

DEMO

Unmasking Malware

RSA
FirstWatch

THANK YOU!!!

BIT.LY/ELISANBOOKS
@TOPHS
FACEBOOK.COM/CCELISAN
LINKEDIN.COM/IN/ELISAN

**Images are copied from the Internet and are owned by their respective authors*