RSA
FIRSTWATCH

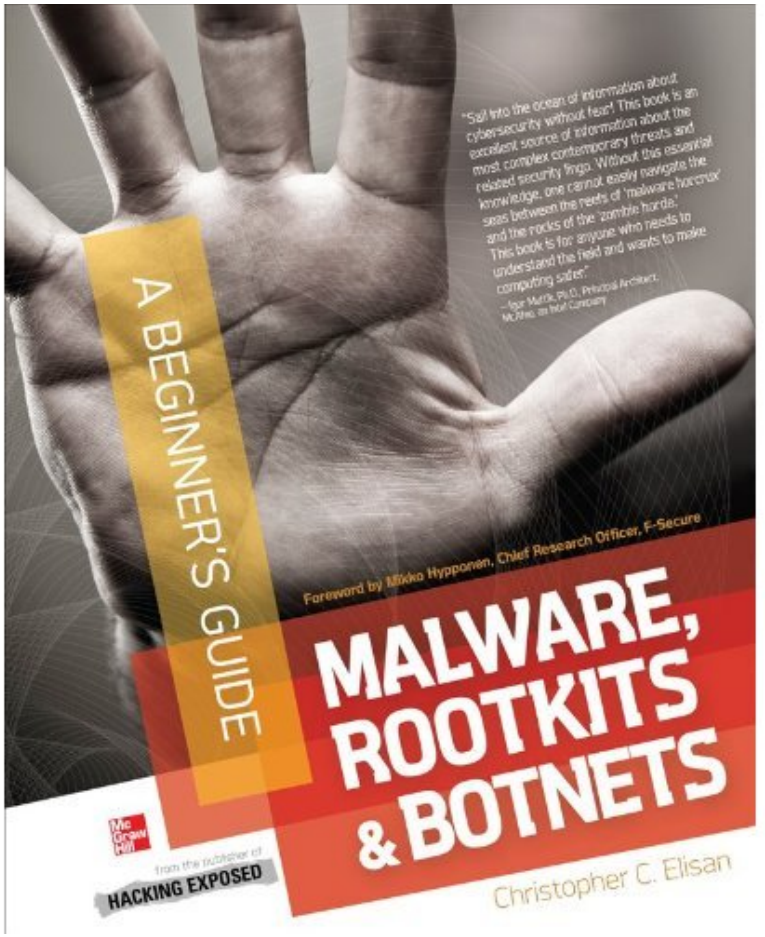
MALWARE AUTOMATION

Christopher C. Elisan
Principal Malware Scientist
RSA NetWitness

RSA FIRSTWATCH

WHO AM I?

- Principal Malware Scientist – RSA NetWitness
- Author of *"Malware, Rootkits & Botnets: A Beginner's Guide"* (*bit.ly/mrbbook*)
- Past Adventures
  - Damballa (2009-2012)
  - F-Secure (2006-2009)
  - Trend Micro (1998-2006)
- @Tophs



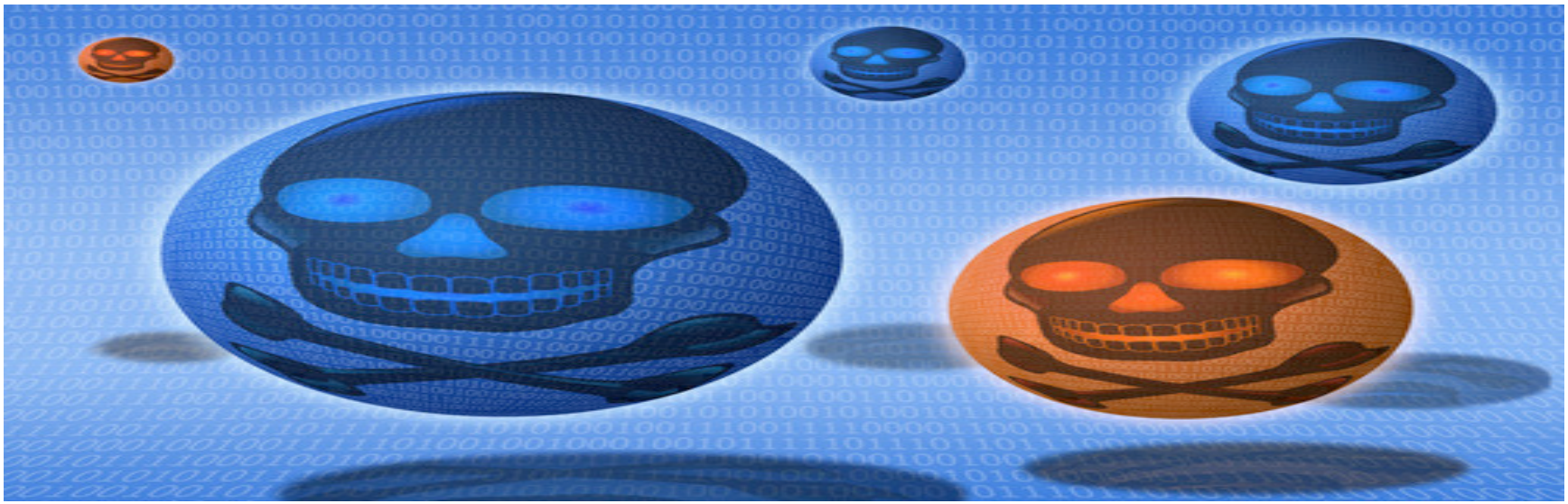
RSA FIRSTWATCH

- RSA's elite, highly trained global threat research and intelligence team
- Provides covert and strategic threat intelligence on advanced threats and actors
- Focuses on unknown threats
- Research operationalized automatically via RSA Live
- @RSAFirstWatch

RSA FIRSTWATCH

PURPOSE OF THE TALK

Understand the tools and methodologies behind the staggering number of malware discovered on a periodic basis…



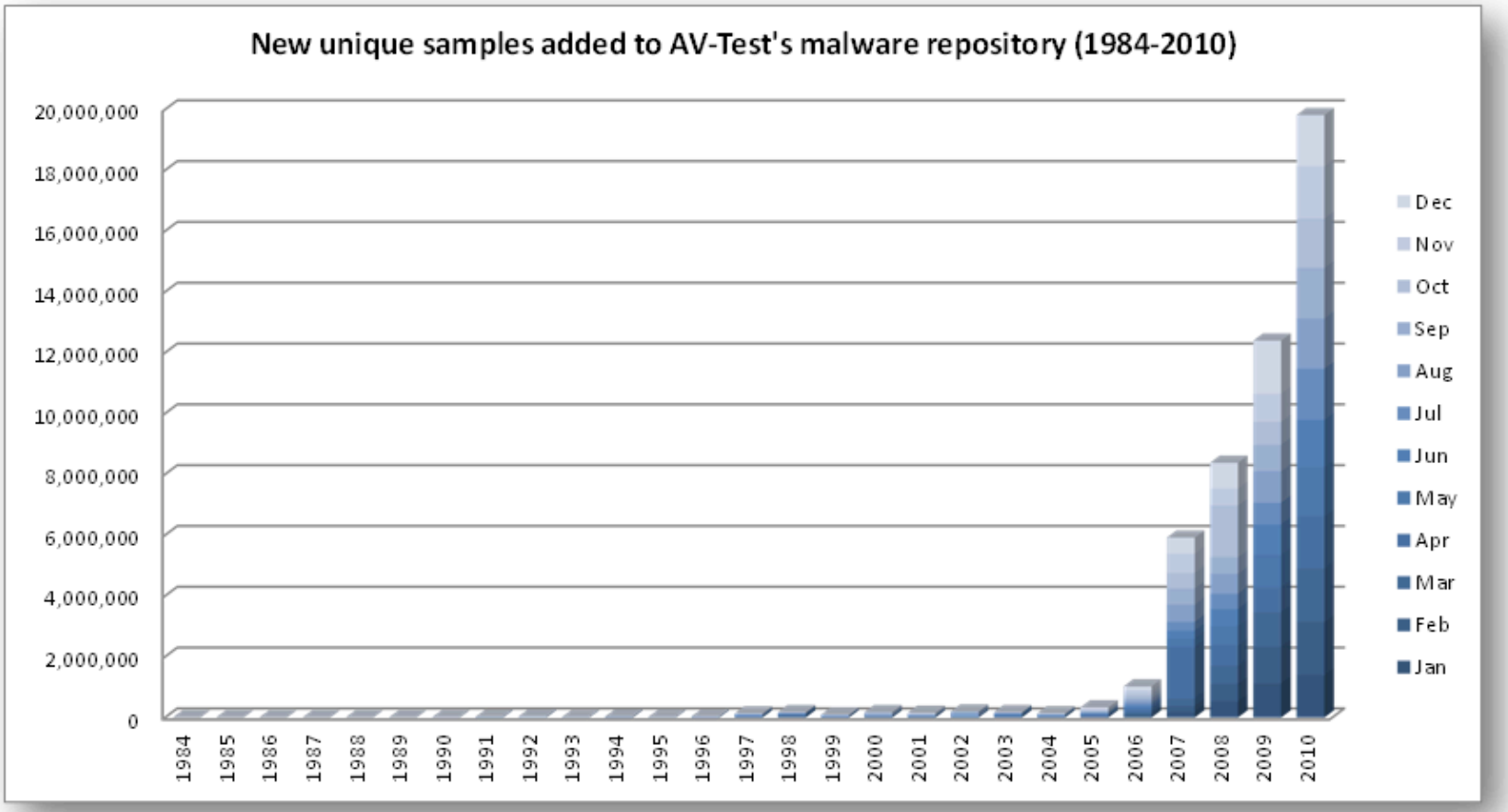
RSA FIRSTWATCH

AGENDA

- What are we up against?
- What are the tools used by attackers?
- How are they doing it?
- Why are they doing it?
- Live Demo

RSA FIRSTWATCH

WE ARE UP AGAINST…



Christopher C. Elisan

RSA
FIRSTWATCH

LONE WOLF

RSA
FIRSTWATCH

ARMY OF ARMORED MALWARE

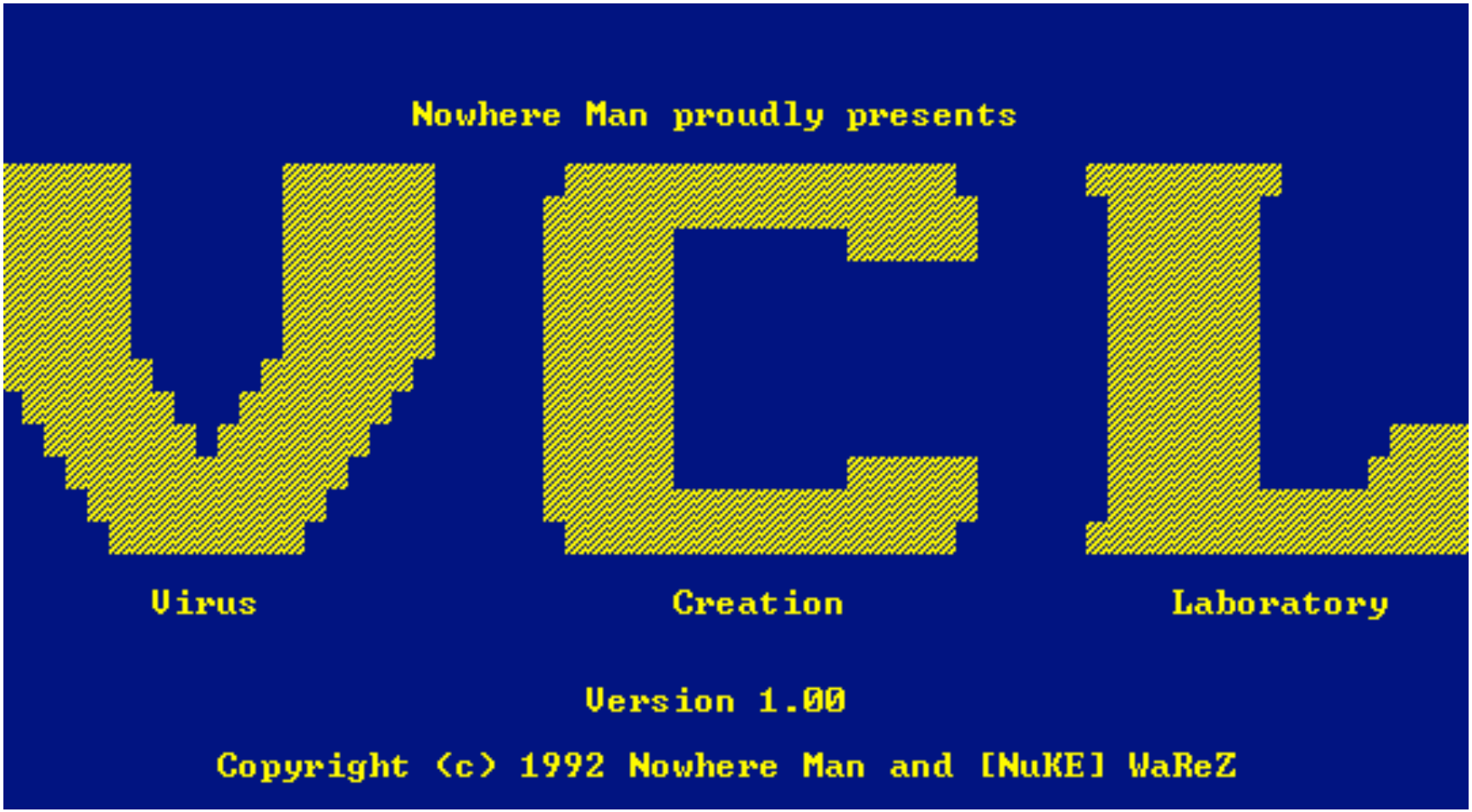
RSA FIRSTWATCH

WHAT?

- DiY Kits
- Armoring Tools
  - Packers
  - Encrypters
  - Joiners / Binders
- AV Scanners
  - On-premise
  - In-the-cloud

RSA
FIRSTWATCH

DIY KITS



RSA
FIRSTWATCH

DIY KITS

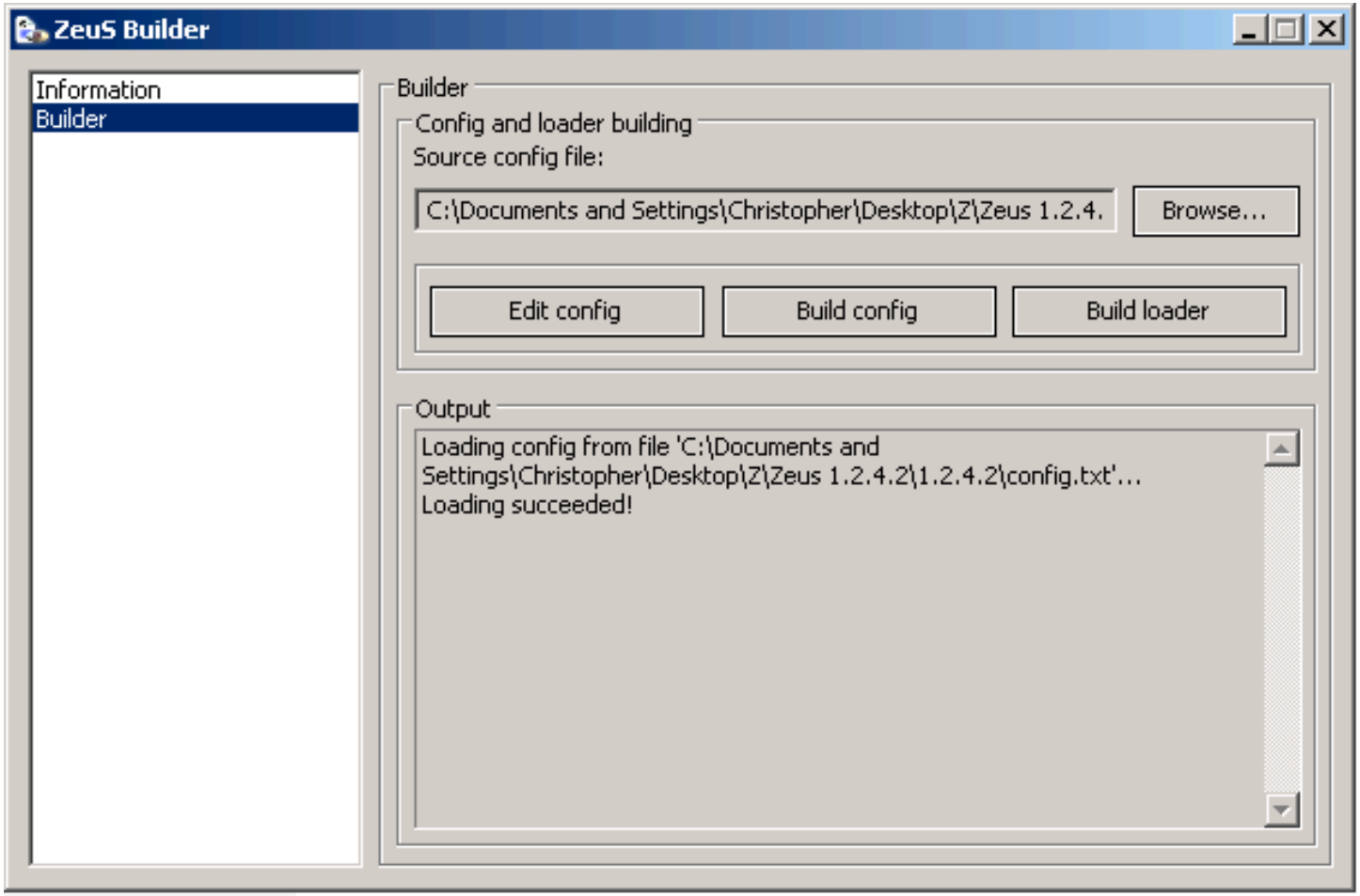
```
PS-MPC ▮ Phalcon/Skism Mass Produced Code Generator
       ▮ Version 0.91β          Written by Dark Angel

Syntax: PS-MPC <file1> <file2> ...
  file1 = name of first configuration file
  file2 = name of second configuration file

Thank you for using the Phalcon/Skism Mass Produced Code Generator
```

RSA
FIRSTWATCH

DIY KITS

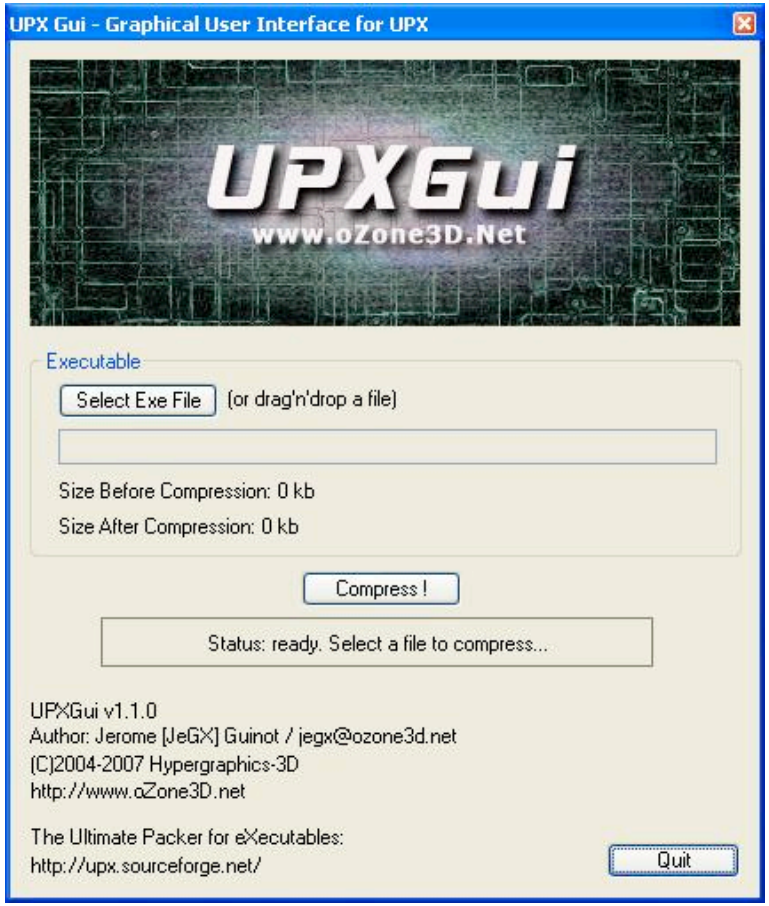
RSA
FIRSTWATCH

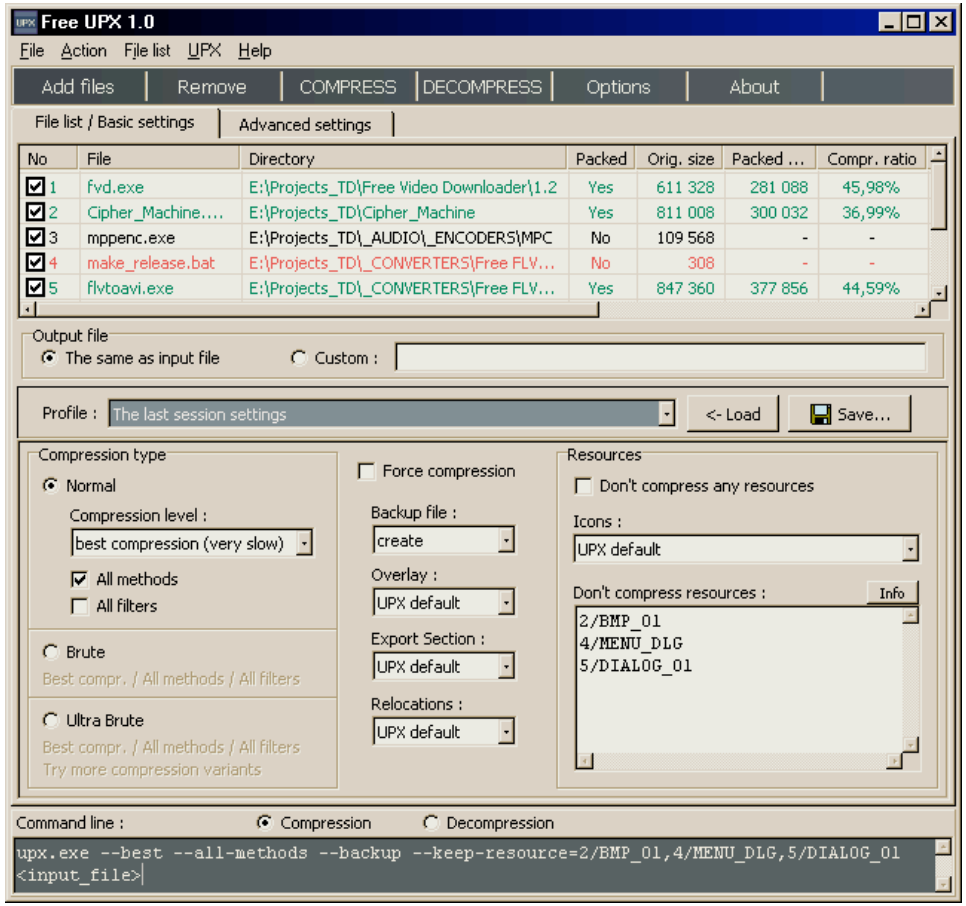
DIY KITS



RSA
FIRSTWATCH

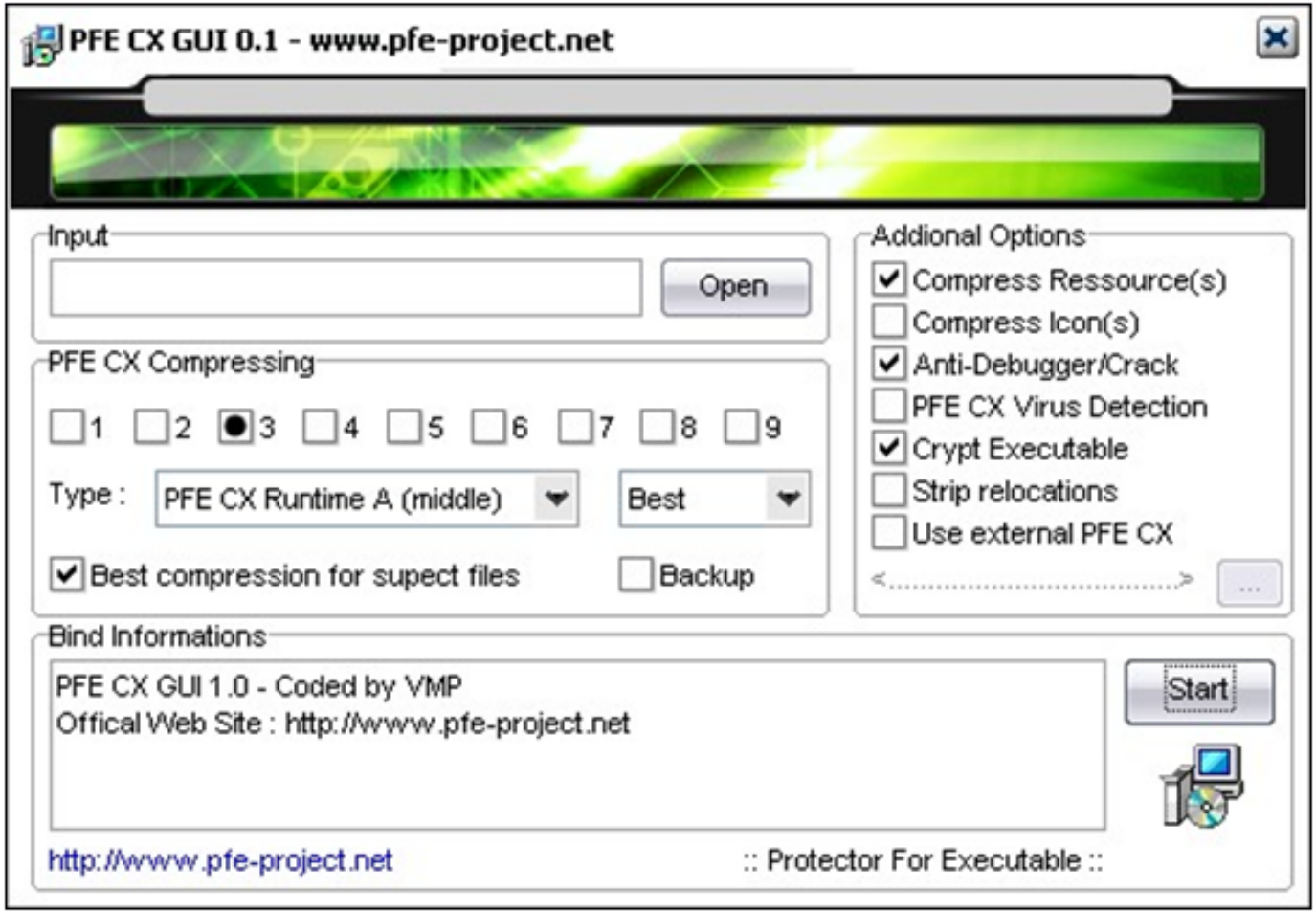
ARMORING TOOLS





RSA
FIRSTWATCH

ARMORING TOOLS



RSA
FIRSTWATCH

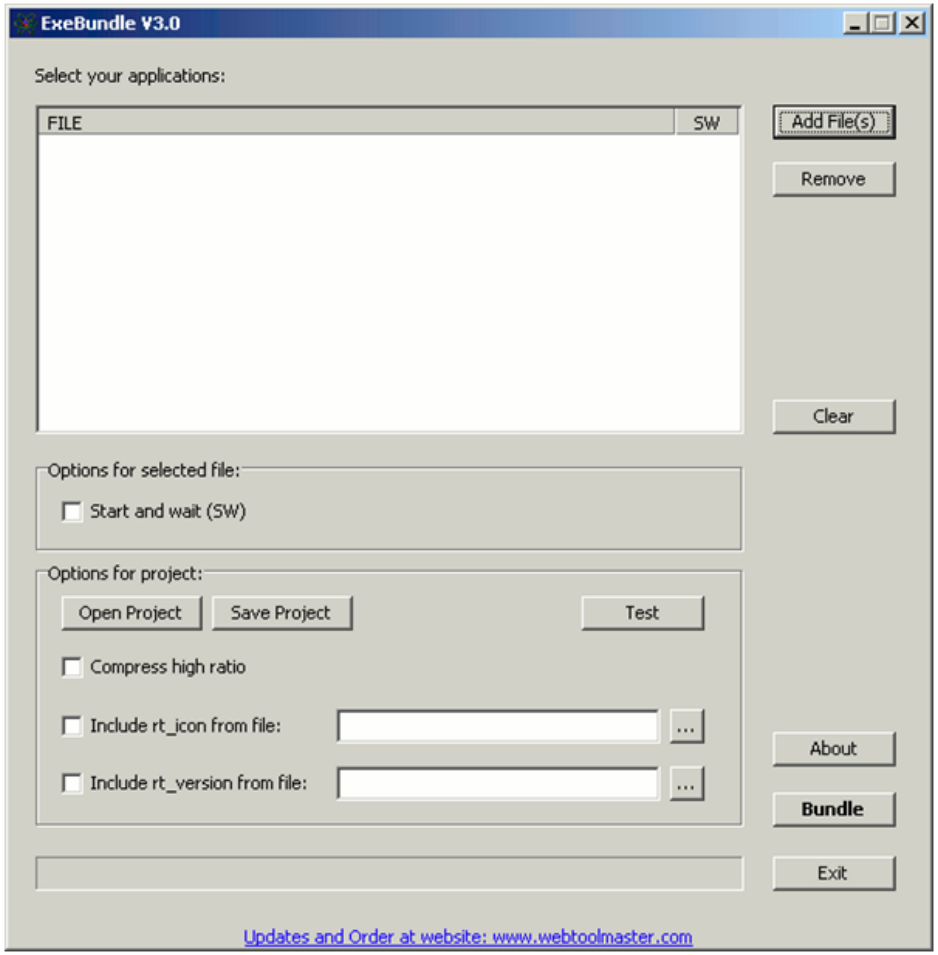
ARMORING TOOLS

RSA FIRSTWATCH

ARMORING TOOLS

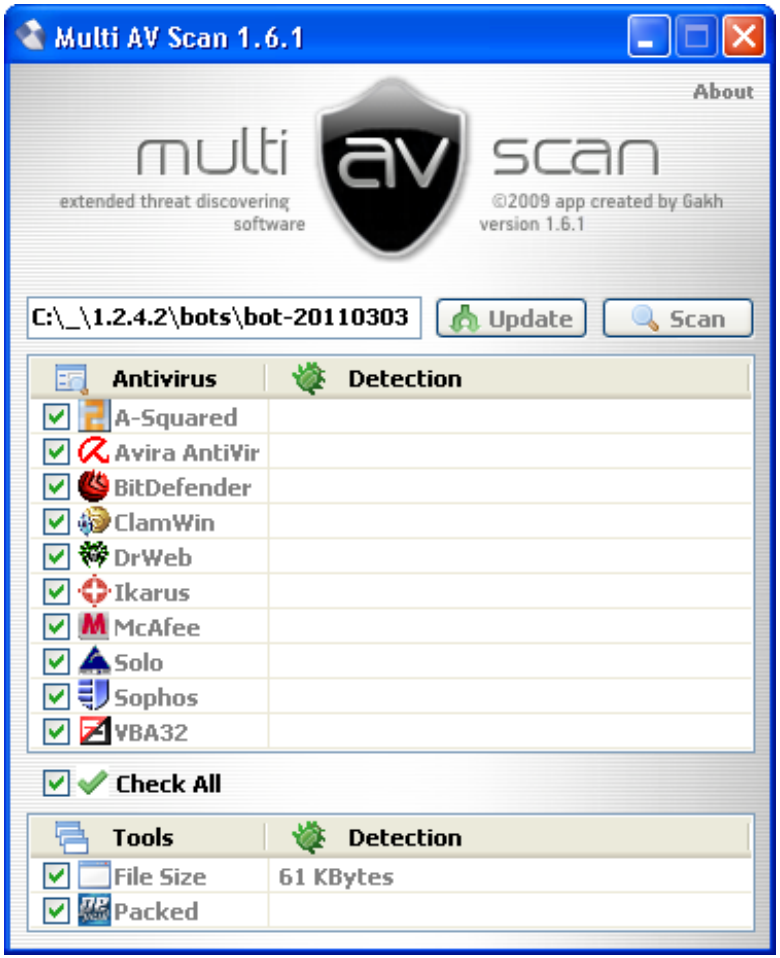
RSA
FIRSTWATCH

ARMORING TOOLS



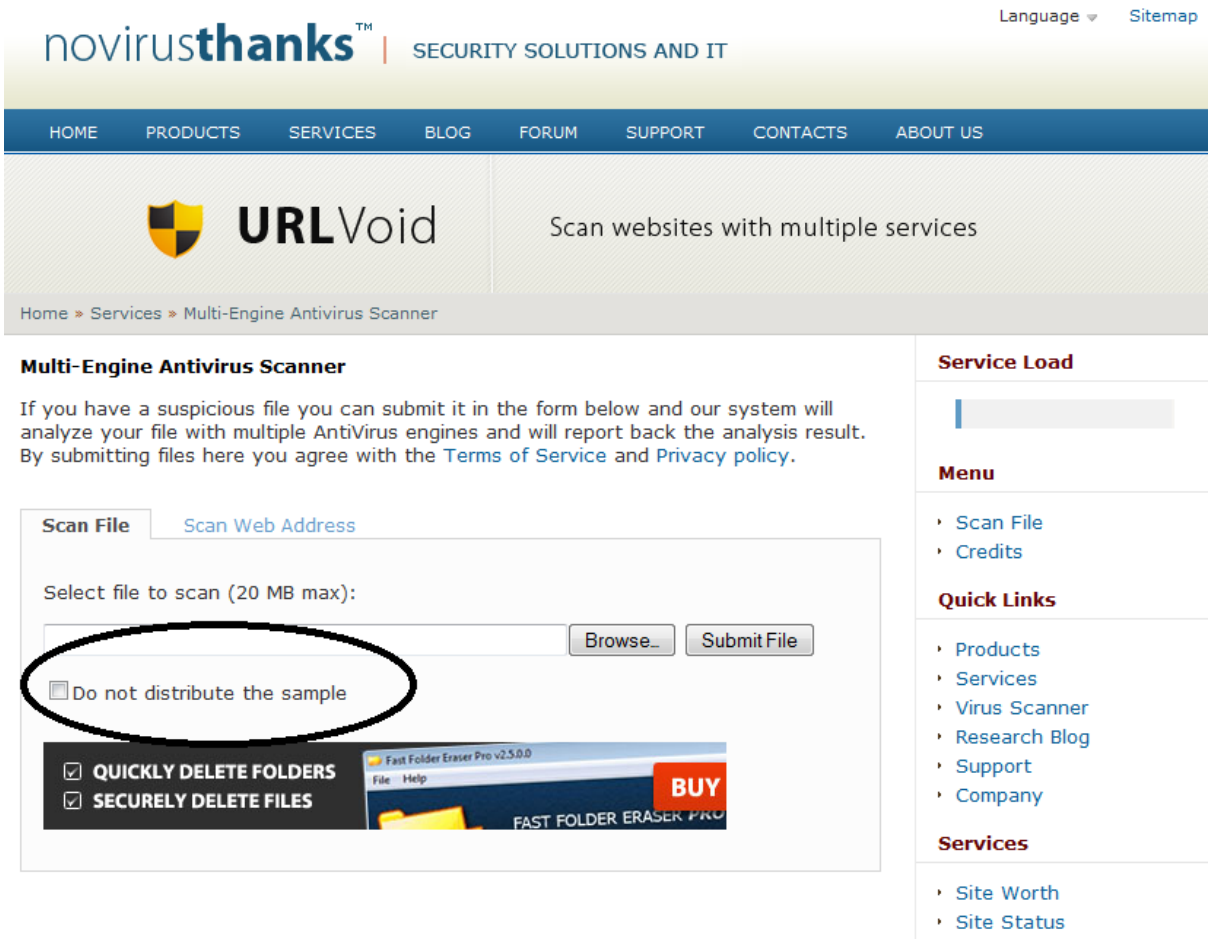
RSA
FIRSTWATCH

AV SCANNERS



RSA FIRSTWATCH

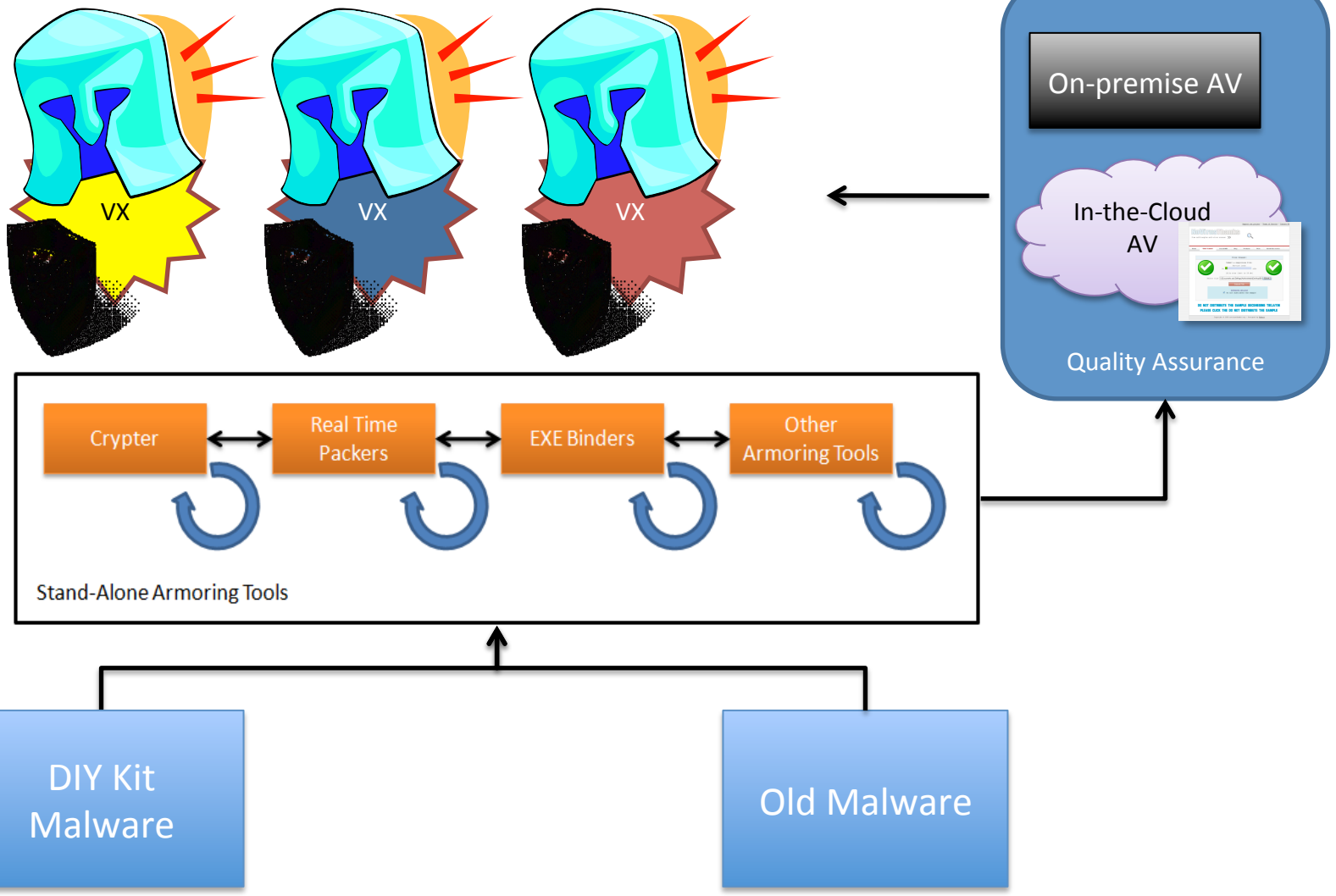
AV SCANNERS



Christopher C. Elisan

RSA FIRSTWATCH

HOW?



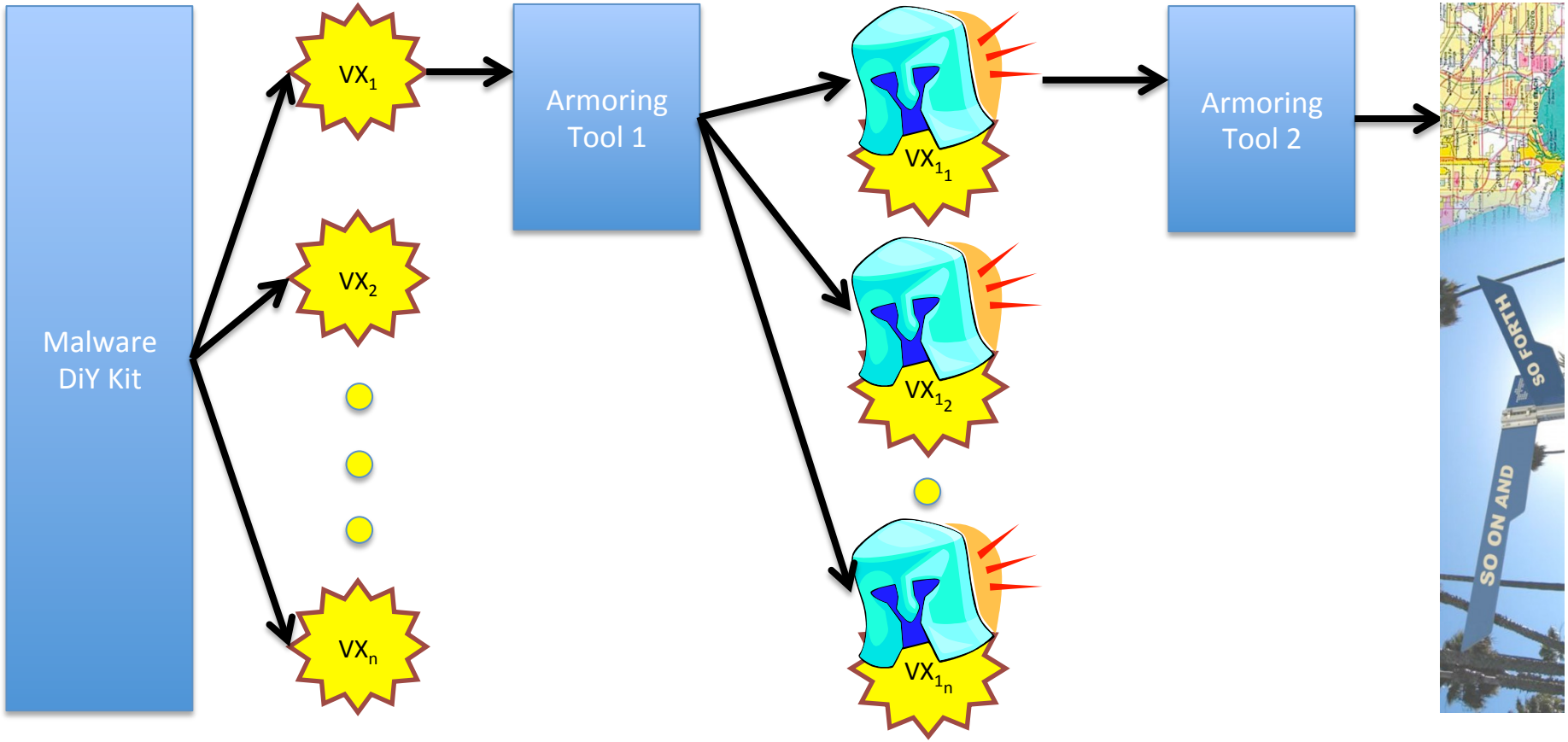
RSA FIRSTWATCH

WHY?

- Exponential effect – strength in numbers
- Easy malware update
- Knock AV Out

RSA FIRSTWATCH

EXPONENTIAL EFFECT



RSA FIRSTWATCH

EASY MALWARE UPDATE

- Unique samples per malware deployment technology
- Malware serving domains can rotate malware in minutes (date and time seed)

RSA FIRSTWATCH

KNOCK AV OUT

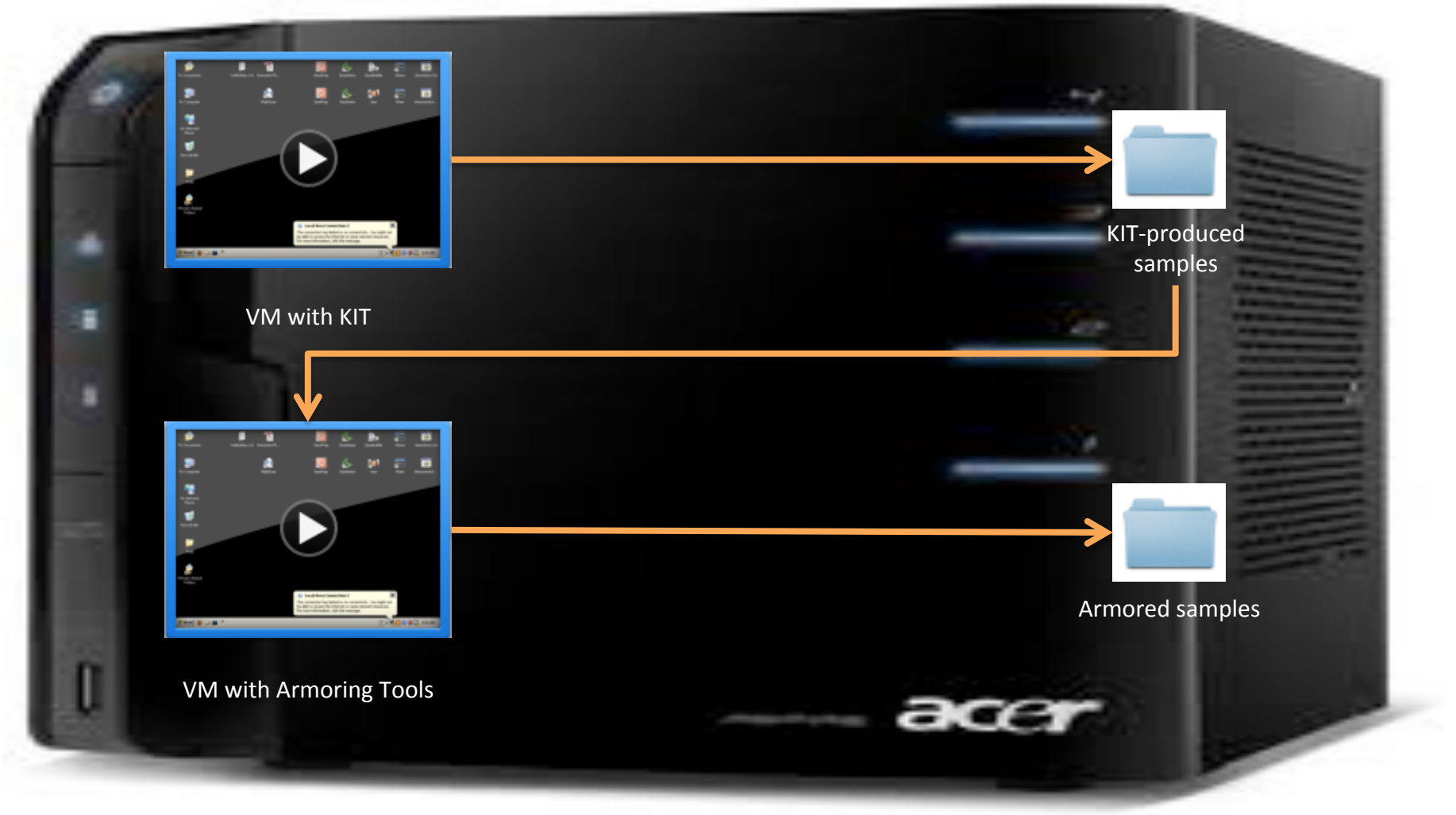
- Malware creation time vs. Solution Cycle time
- AV evasion effectively utilized
- 1:1 signature ratio
- Understanding the malware requires reversing and not just analysis

RSA

FIRSTWATCH

RSA FirstWatch

PUTTING THEM TOGETHER



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

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

Christopher C. Elisan