

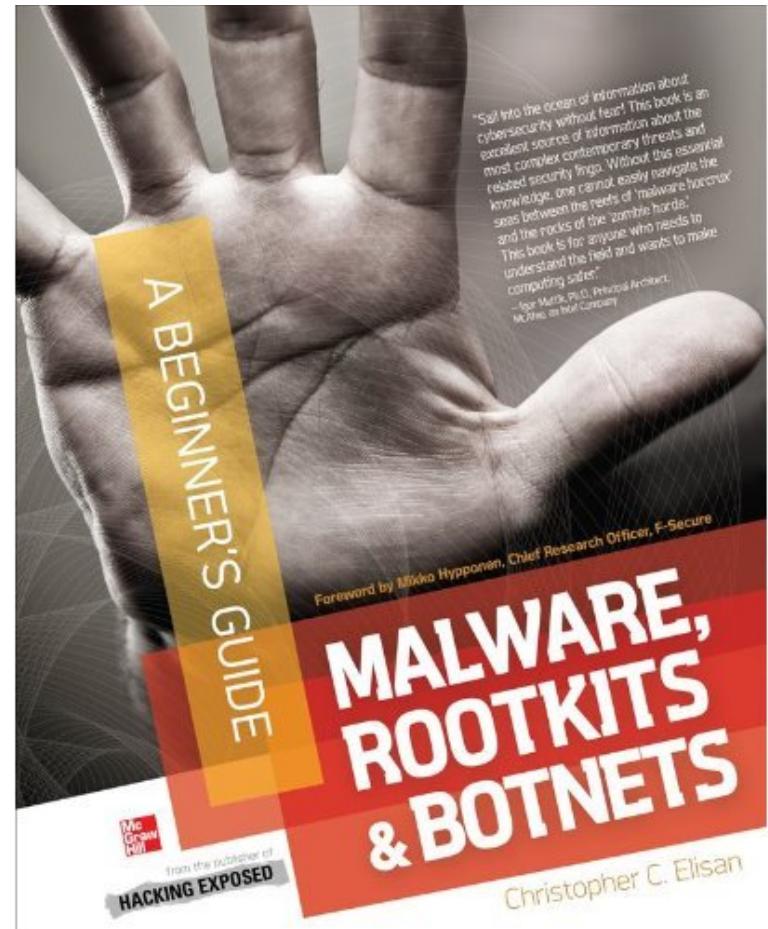


MALWARE AUTOMATION

Christopher C. Elisan
Principal Malware Scientist
RSA NetWitness

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

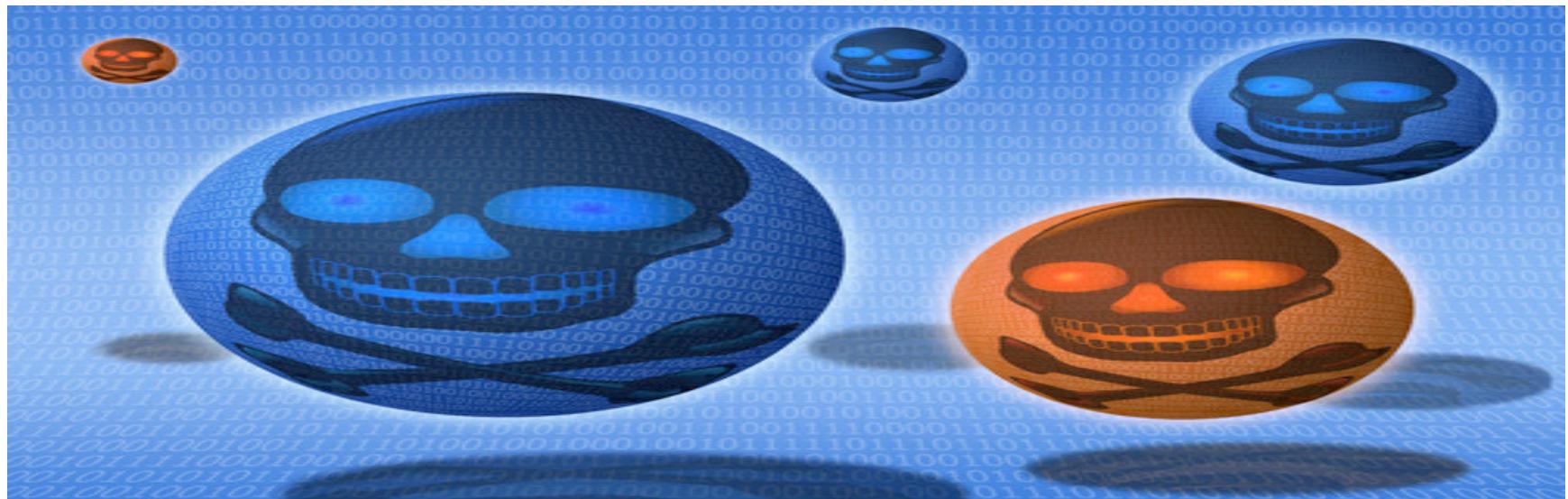
- RSA's elite, highly trained global threat research and intelligence team
- Provides covert and strategic threat intelligence on advanced threats and actors
- Focuses on unknown threats
- Research operationalized automatically via RSA Live
- @RSAFirstWatch



PURPOSE OF THE TALK

LOOKING AT THE DATA

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



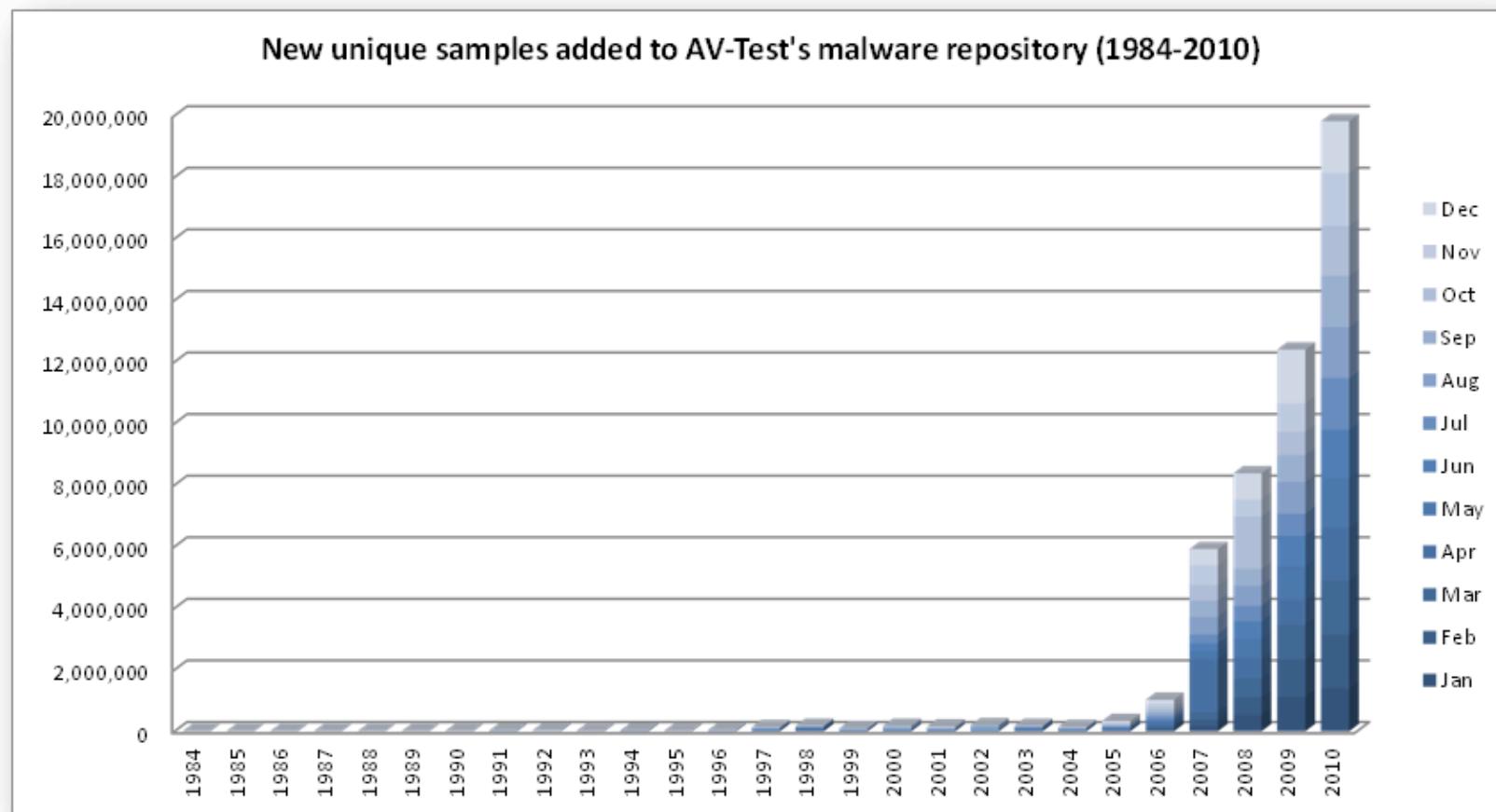


AGENDA

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

WE ARE UP AGAINST...



RSA

FIRSTWATCH

LONE WOLF



RSA

FIRSTWATCH

ARMY OF ARMORED MALWARE



WHAT?

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



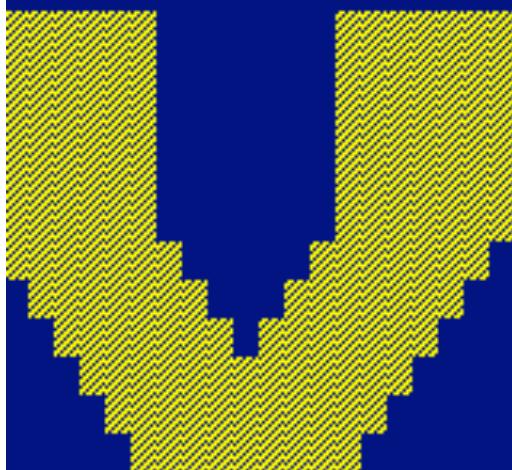
RSA

FIRSTWATCH

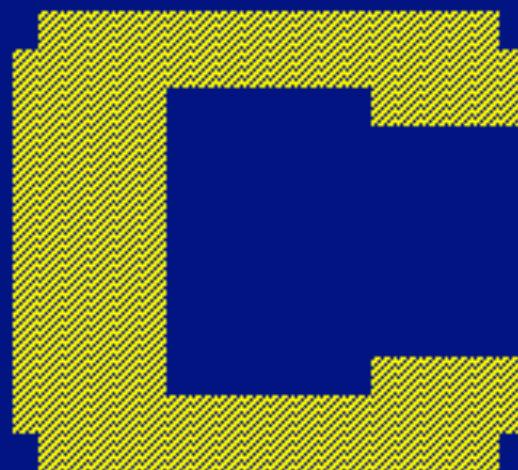
DIY KITS

DIY KITS

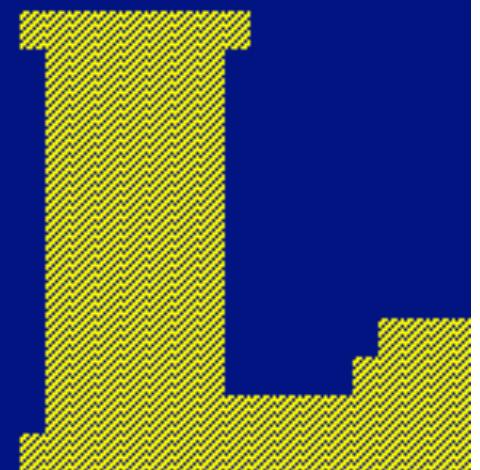
Nowhere Man proudly presents



Virus



Creation



Laboratory

Version 1.00

Copyright (c) 1992 Nowhere Man and [NuKE] WaReZ

RSA

FIRSTWATCH

DIY KITS

DLL MID

PS-MPC | Phalcon/Skism Mass Produced Code Generator
| Version 0.910 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

DIY KITS

DIY KITS



Spy Eye v1.0

Path to the main control panel:

Alternative path to the main control panel:

Path to the formgrabber control panel:

Encryption key:

Connector interval (sec):

Compress build by UPX v3.04w:

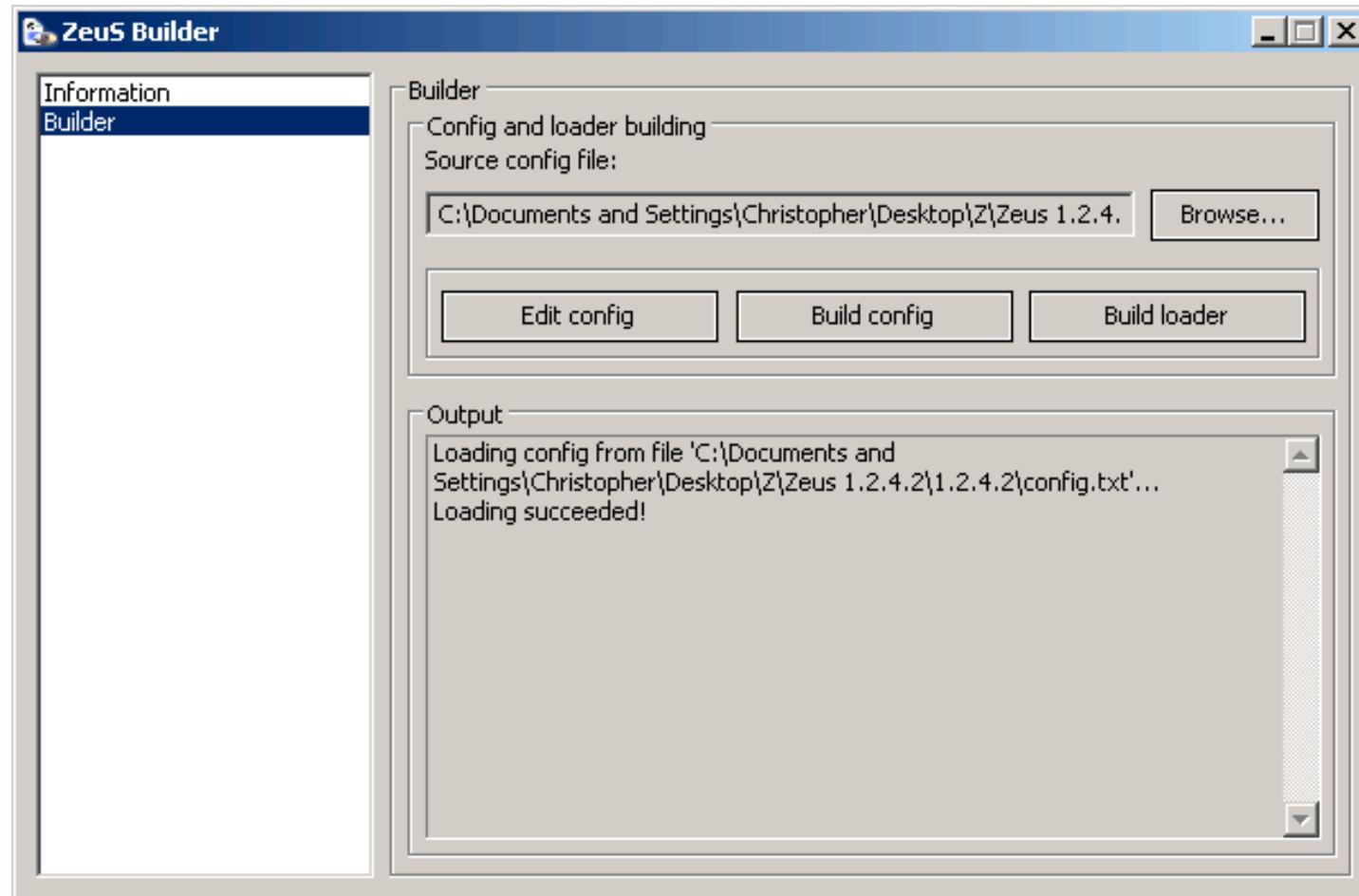
Kill Zeus:

Make config & get build **Get build**

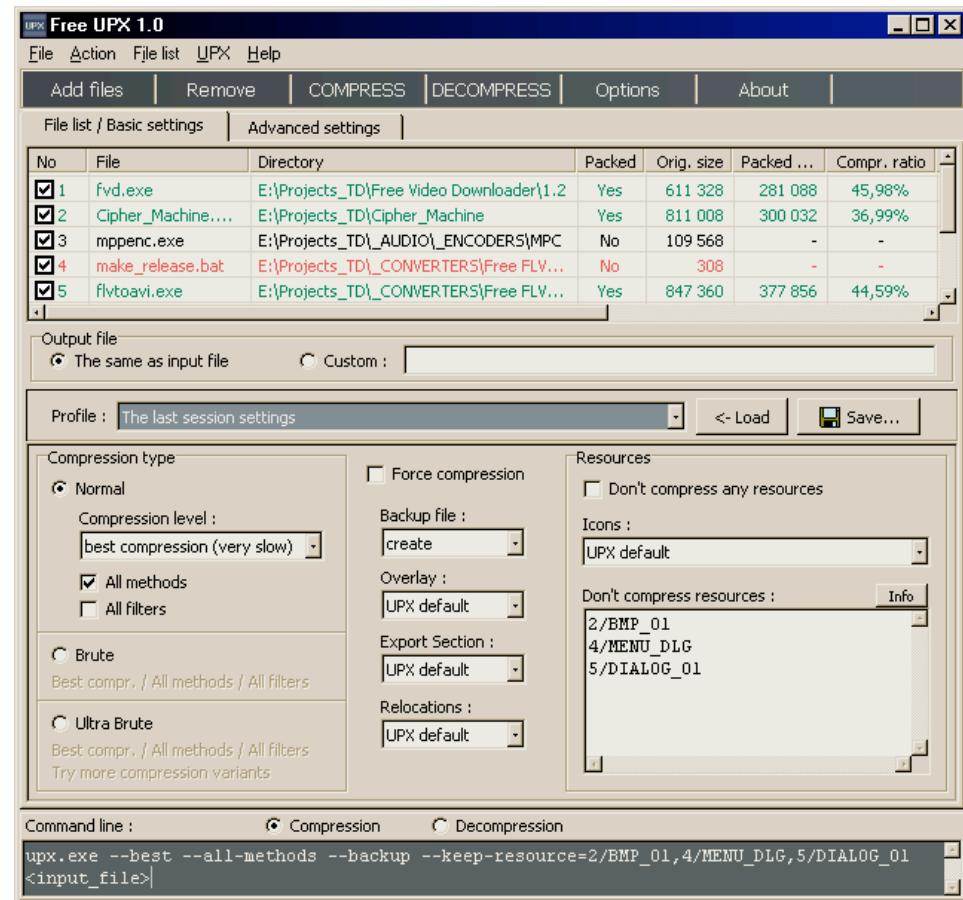
Are you infected by SpyEye?
Your system is clean

DIY KITS

DIY KITS

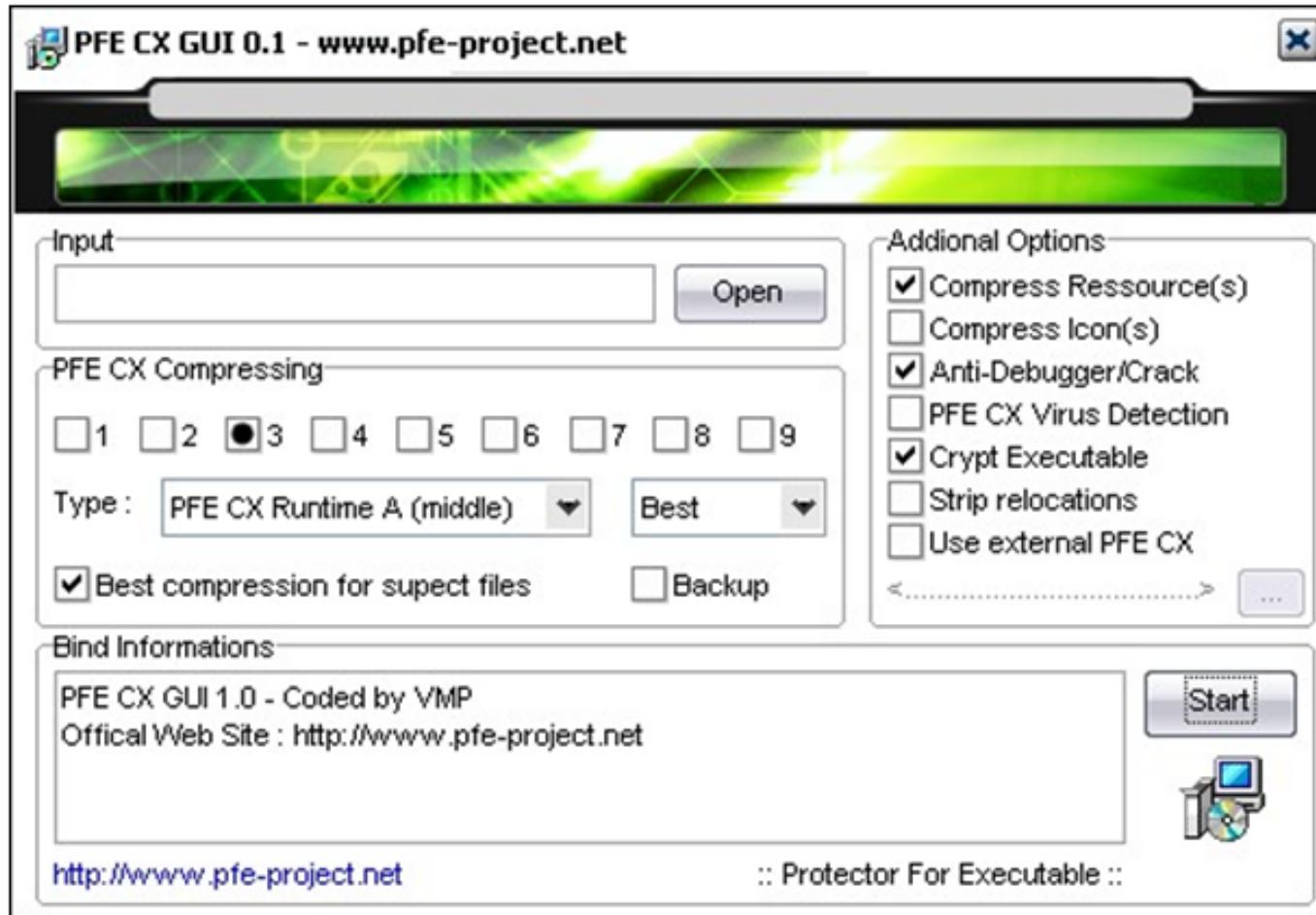


ARMORING TOOLS



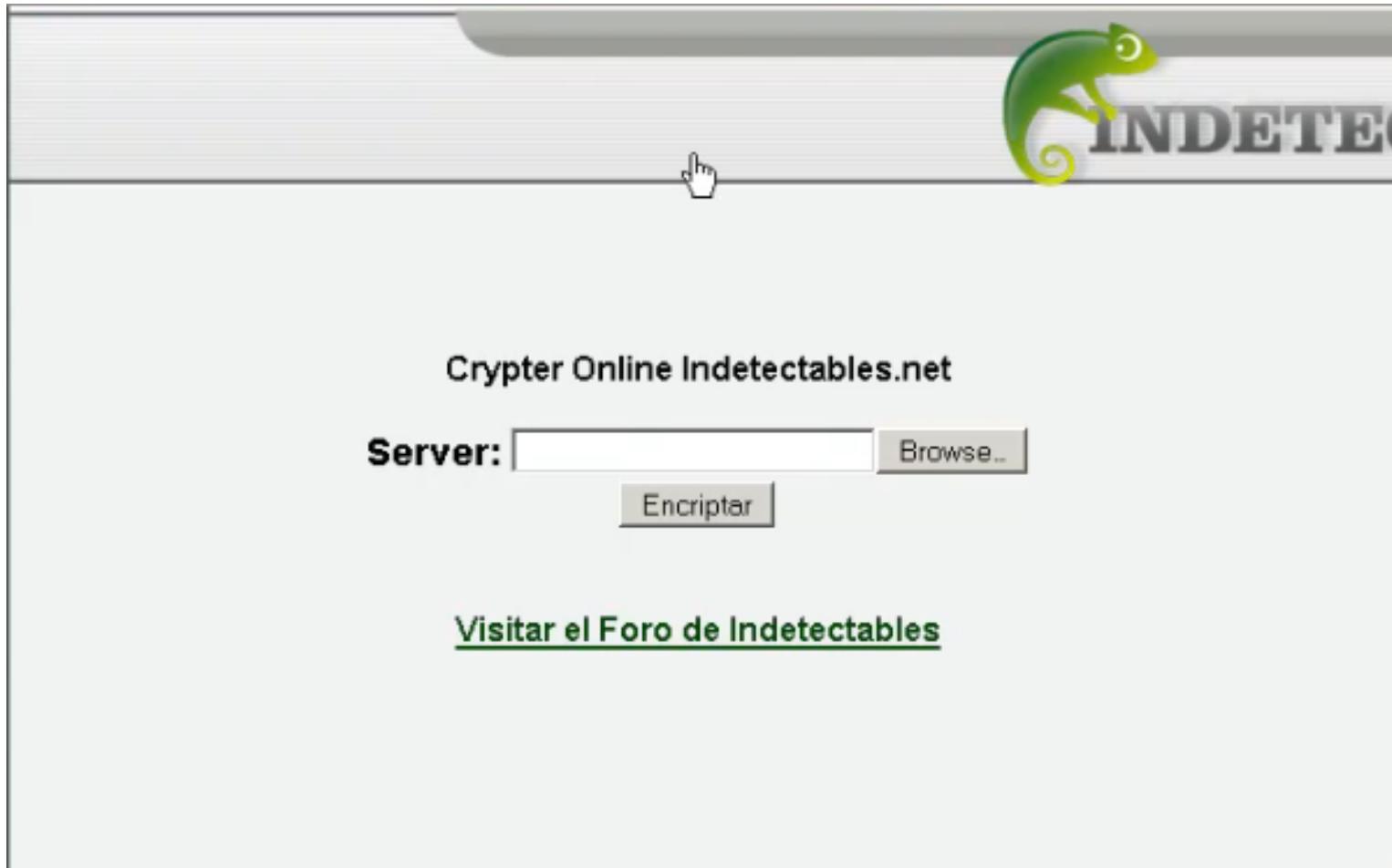
ARMORING TOOLS

WUWOKWIAI LOOF2





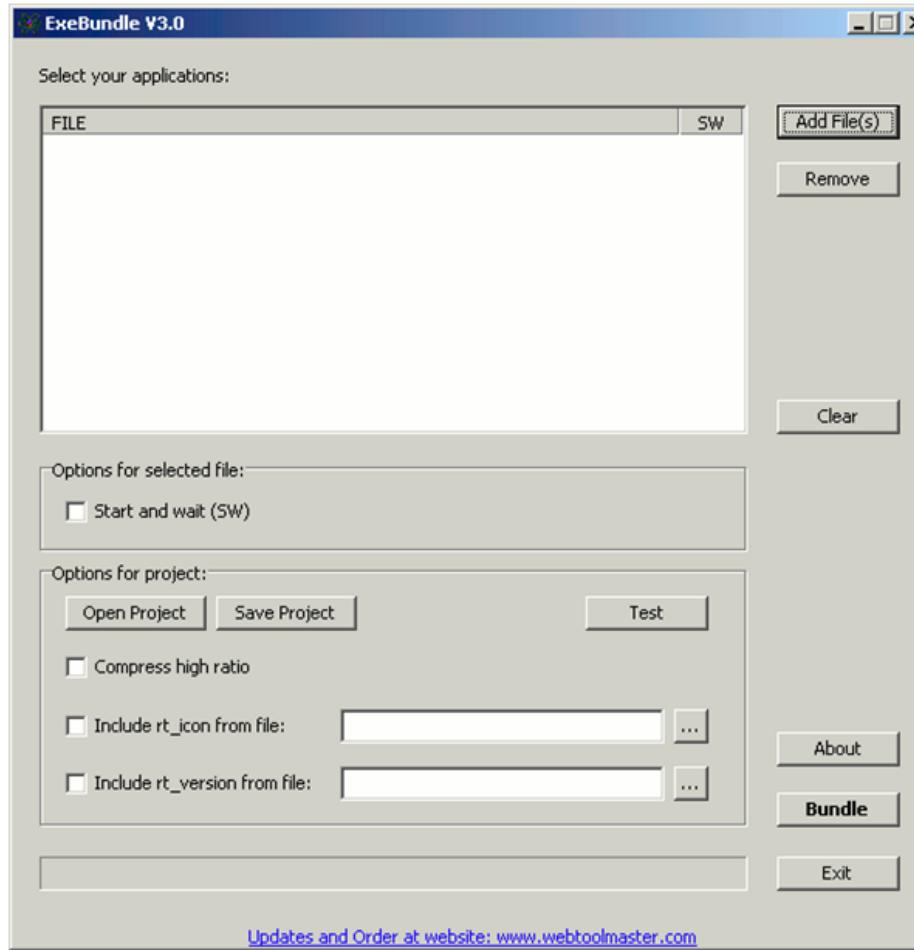
ARMORING TOOLS



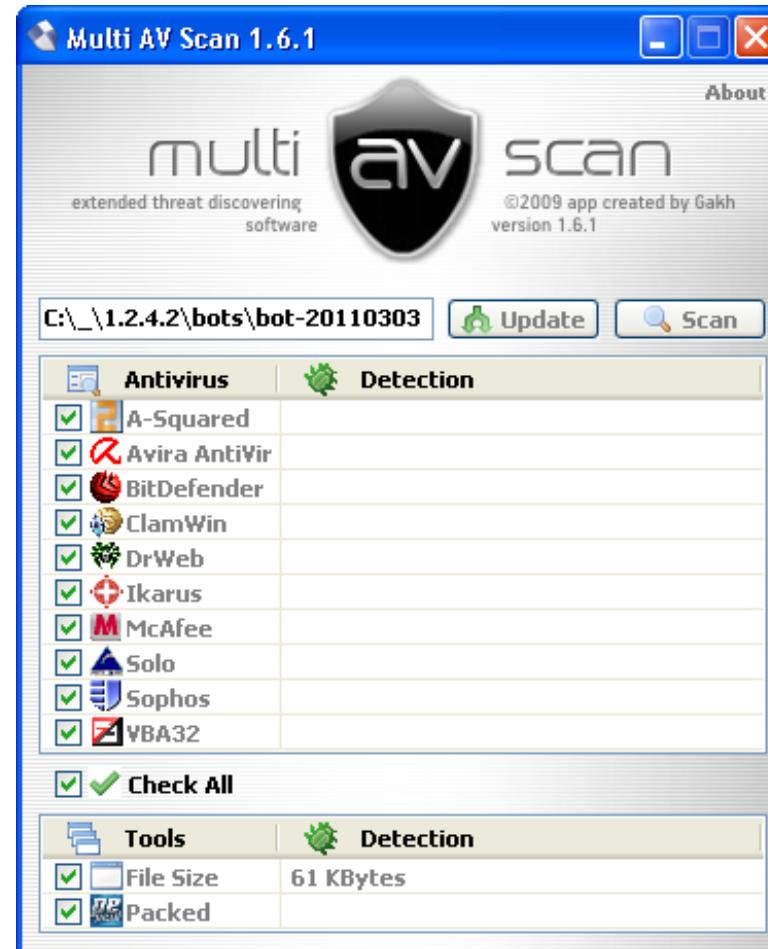
ARMORING TOOLS



ARMORING TOOLS



AV SCANNERS



AV SCANNERS

novirus**thanks**™ | SECURITY SOLUTIONS AND IT

Language ▾ Sitemap

HOME PRODUCTS SERVICES BLOG FORUM SUPPORT CONTACTS ABOUT US



URLVoid

Scan websites with multiple services

Home » Services » Multi-Engine Antivirus Scanner

Multi-Engine Antivirus Scanner

If you have a suspicious file you can submit it in the form below and our system will analyze your file with multiple AntiVirus engines and will report back the analysis result. By submitting files here you agree with the [Terms of Service](#) and [Privacy policy](#).

Scan File

Scan Web Address

Select file to scan (20 MB max):

[Browse...](#)

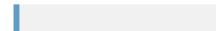
[Submit File](#)

Do not distribute the sample

QUICKLY DELETE FOLDERS
 SECURELY DELETE FILES



Service Load



Menu

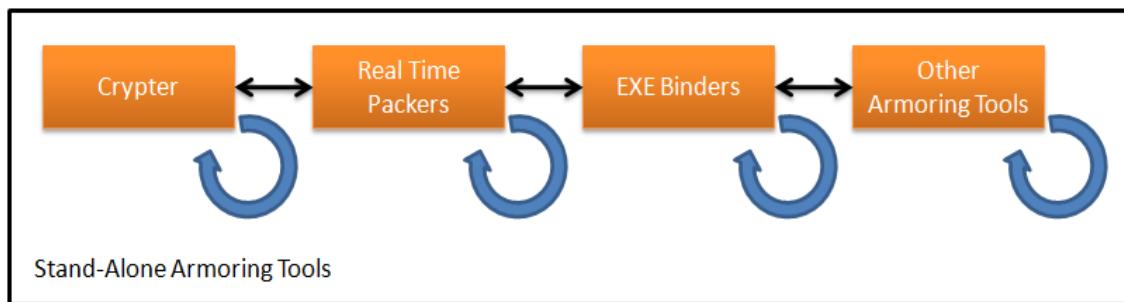
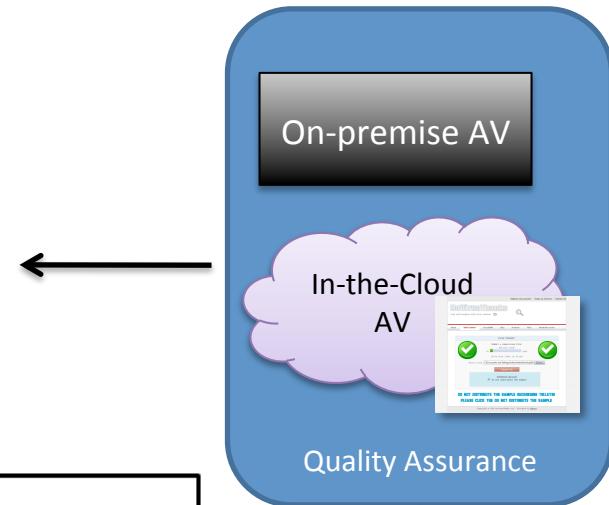
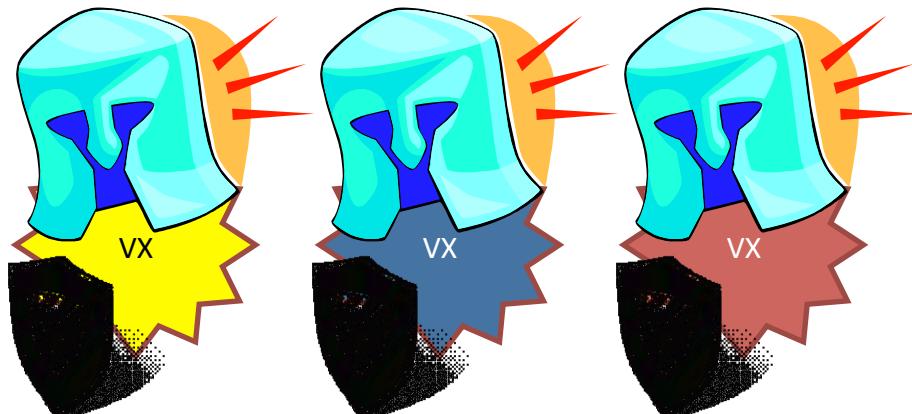
- › [Scan File](#)
- › [Credits](#)

Quick Links

- › [Products](#)
- › [Services](#)
- › [Virus Scanner](#)
- › [Research Blog](#)
- › [Support](#)
- › [Company](#)

Services

- › [Site Worth](#)
- › [Site Status](#)

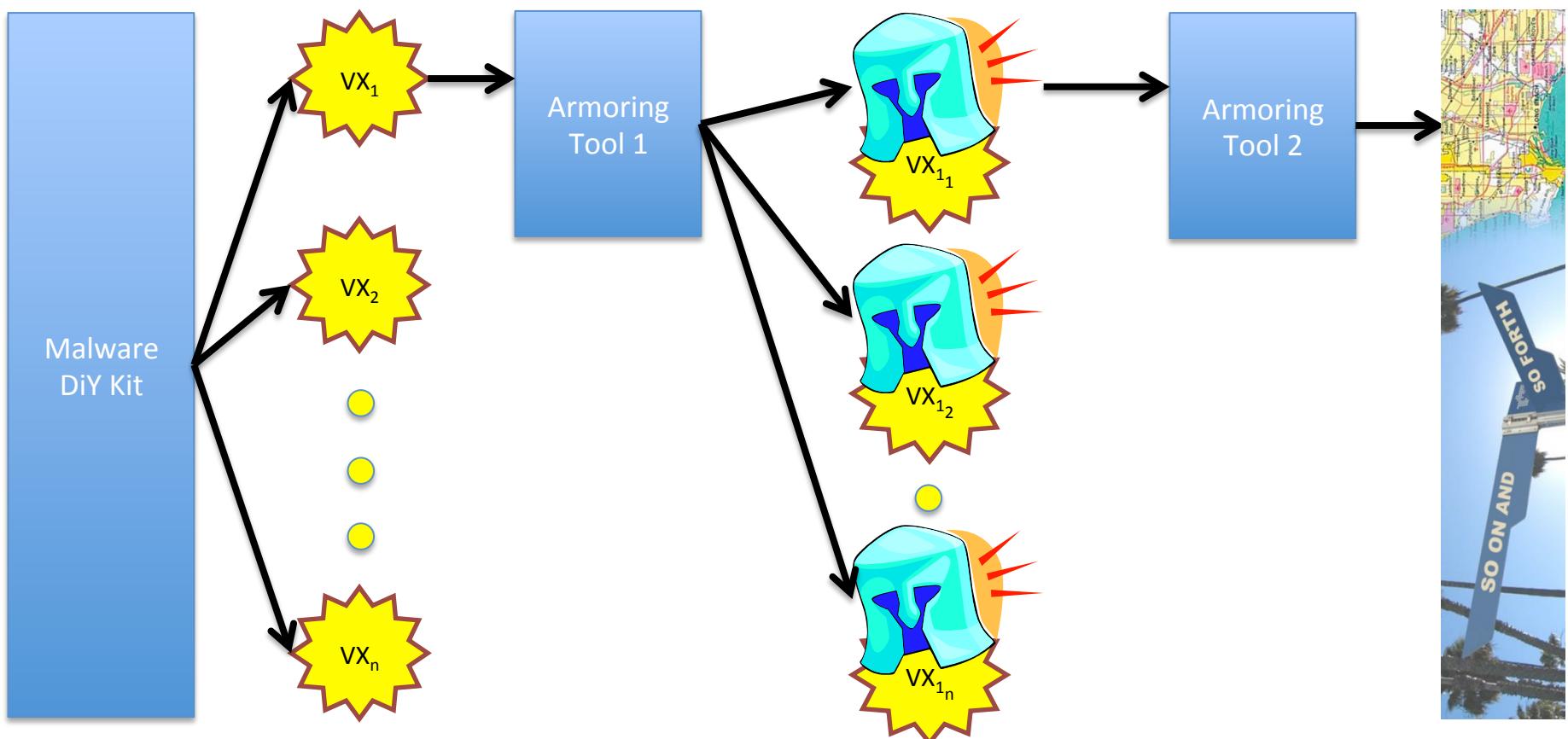


WHY?

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



EXPONENTIAL EFFECT



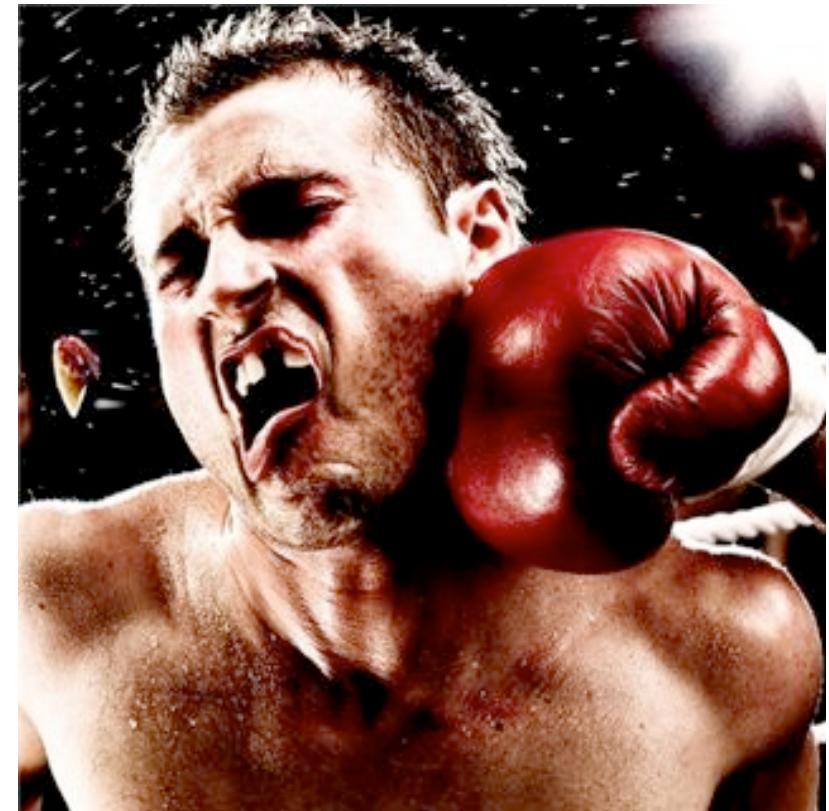
EASY MALWARE UPDATE

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



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



PUTTING THEM TOGETHER

Joining KIT and Armored





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

