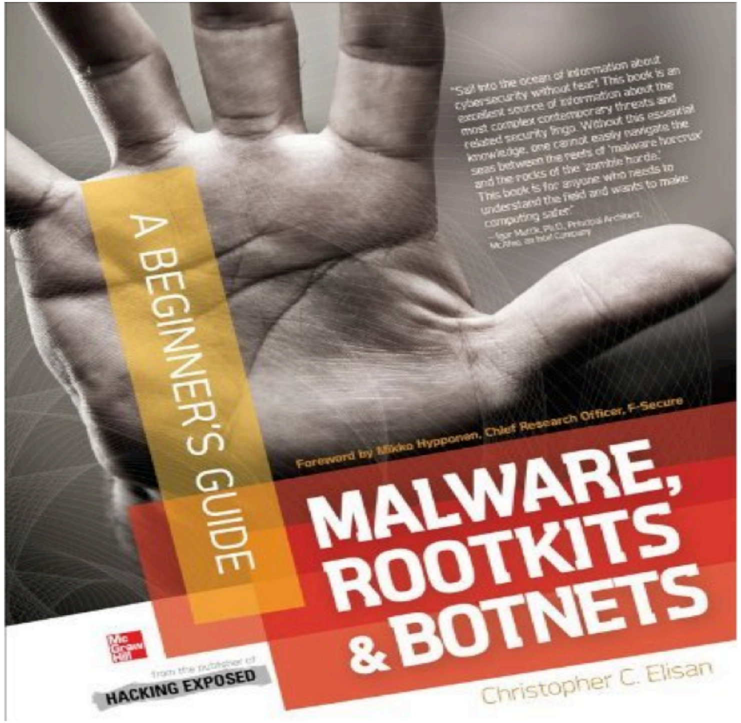
Demystifying a Malware Attack

Christopher Elisan
Principal Malware Scientist
RSA

About Me

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

Author of



"Sail into the ocean of information about cybersecurity without fear! This book is an excellent source of information about the most complex contemporary threats and related security lingo. Without this essential knowledge, one cannot easily navigate the seas between the reefs of 'malware horcrux' and the rocks of the 'zombie horde.' This book is for anyone who needs to understand the field and wants to make computing safer."

—Igor Muttik, Ph.D., Principal Architect, McAfee, an Intel Company

A BEGINNER'S GUIDE

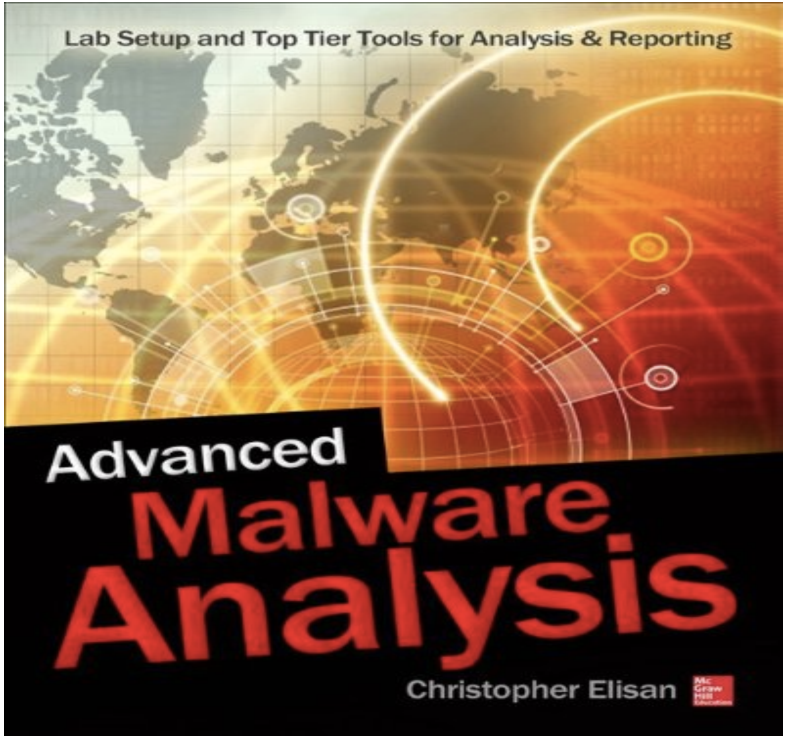
Foreword by Mikko Hypponen, Chief Research Officer, F-Secure

MALWARE, ROOTKITS & BOTNETS

Christopher C. Elisan

from the publisher of HACKING EXPOSED

2012



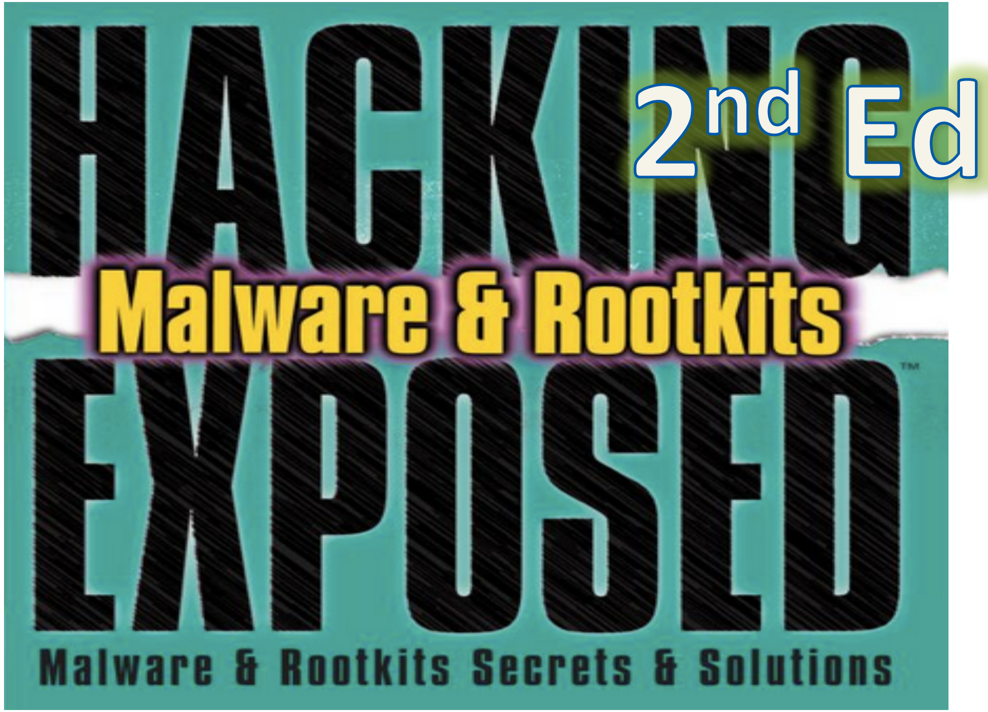
Lab Setup and Top Tier Tools for Analysis & Reporting

Advanced Malware Analysis

Christopher Elisan

2015

Co-Author of



HACKING

Malware & Rootkits

EXPOSED™

Malware & Rootkits Secrets & Solutions

2nd Edition

2016

Agenda

- The Attack
- Behind the Scenes
- Lessons Learned

The Attack

We Are All Under Attack

OPPORTUNISTIC

TARGETED

Opportunistic Attack

Opportunistic Attack

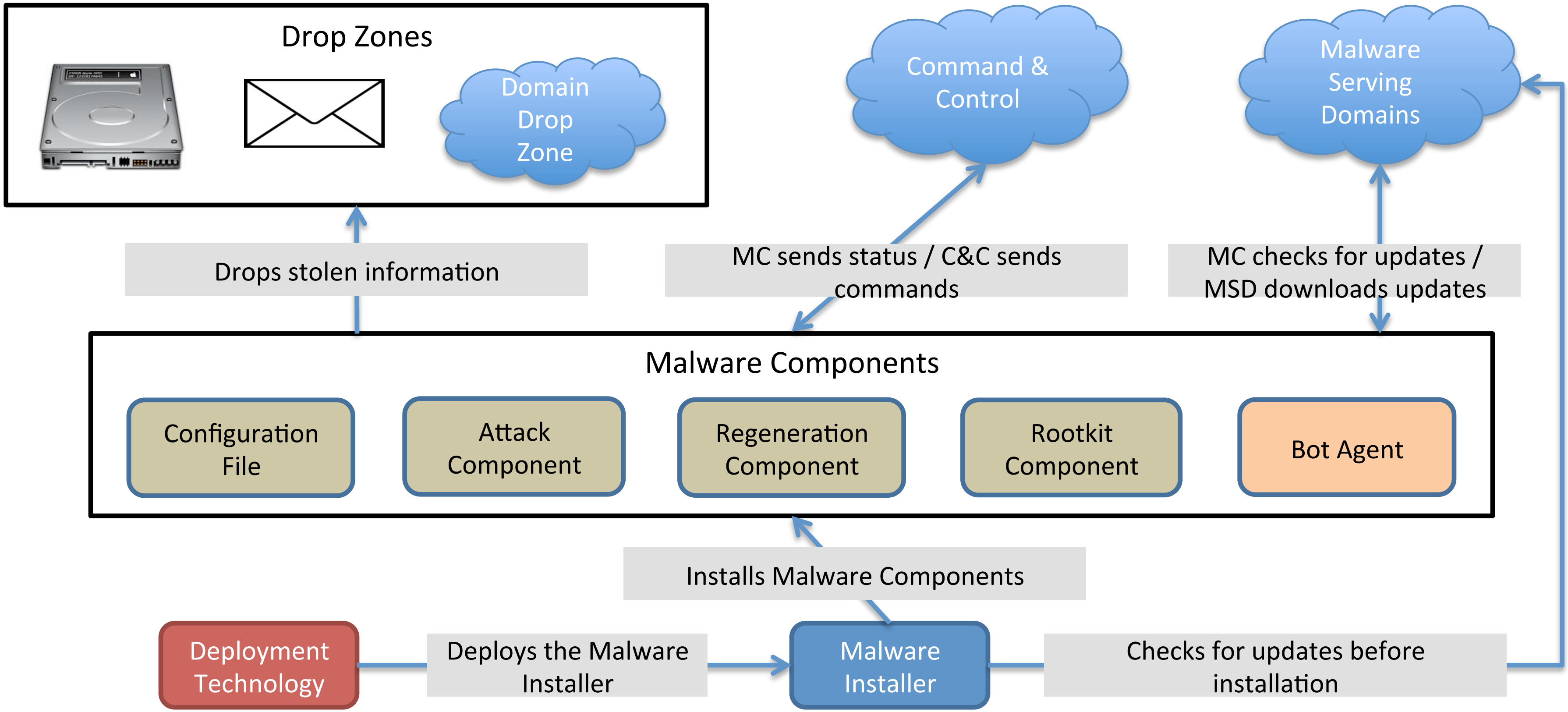
Opportunistic Attack

Targeted Attack

Regardless of the attack, the threat infrastructure and the people behind them are similar

Behind the Scenes

Attack Infrastructure



The Attackers

Sponsor
- Government
- Commercial Organization
- Non-commercial Organization
- Activist Groups
- Individual
- Terrorist Organization

Crime Boss
- Runs the show
- Individual or organization
- Middle man between sponsor and TPs
- Can be a sponsor

Money Mules
- Unsuspecting Public
- Work from home

Malware Writers
- Original malware creator(s)
- Offer malware “off-the-rack” or custom built
- May offer DIY construction kits
- Money-back guarantee if detected
- 24x7 support

Botnet Master
- Individual or criminal team that owns the botnet
- Maintains and controls the botnet
- Holds admin credentials for CnC

Botnet Operator
- Operates a section of the botnet for direct financial gain
- Issues commands to the bot agents
- May be the **Botnet** Master

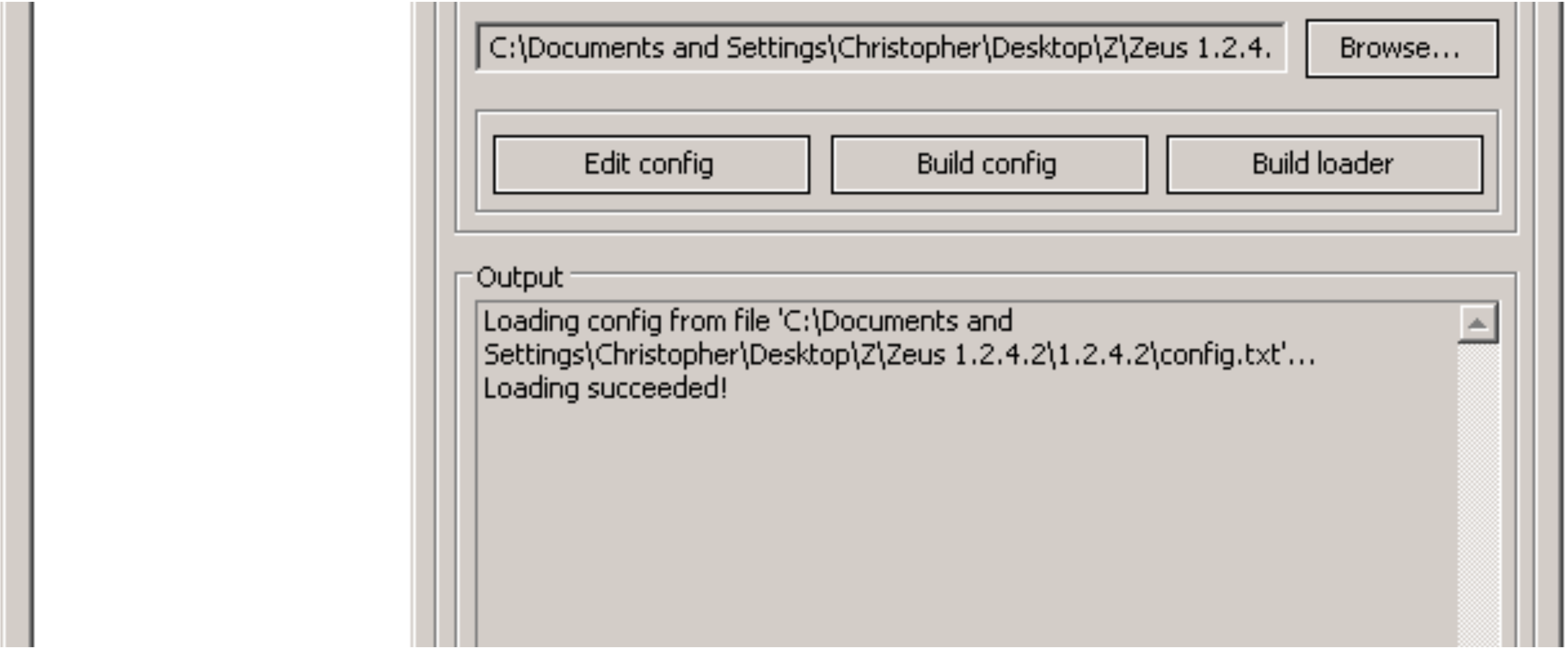
Deployment Provider
- Specialized distribution network
- Attracts and infects victims
- Global & targeted content delivery
- Delivery through Spam/drive-by/USB/etc.
- Offers 24x7 support

Resilience Provider (MSP)
- Provides CnC resilience services
- Anti-takedown network construction
- Bullet-proof domain hosting
- Fast-flux DNS services
- Offers 24x7 Support

Malware Tools

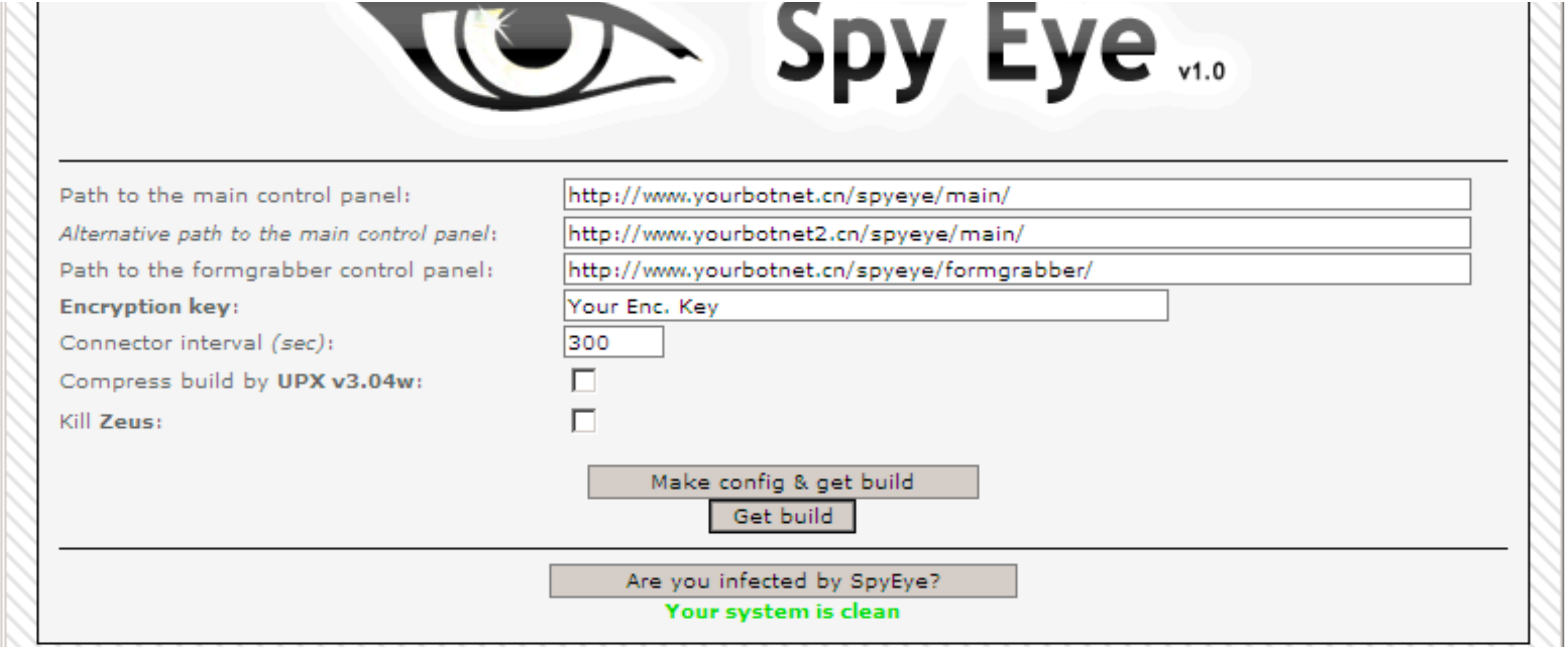
- DiY Kits
- Armoring Tools

DiY Kits



```
Loading config from file 'C:\Documents and
Settings\Christopher\Desktop\Z\Zeus 1.2.4.2\1.2.4.2\config.txt'...
Loading succeeded!
```

DiY Kits



Path to the main control panel: http://www.yourbotnet.cn/spyeye/main/

Alternative path to the main control panel: http://www.yourbotnet2.cn/spyeye/main/

Path to the formgrabber control panel: http://www.yourbotnet.cn/spyeye/formgrabber/

Encryption key: Your Enc. Key

Connector interval *(sec)*: 300

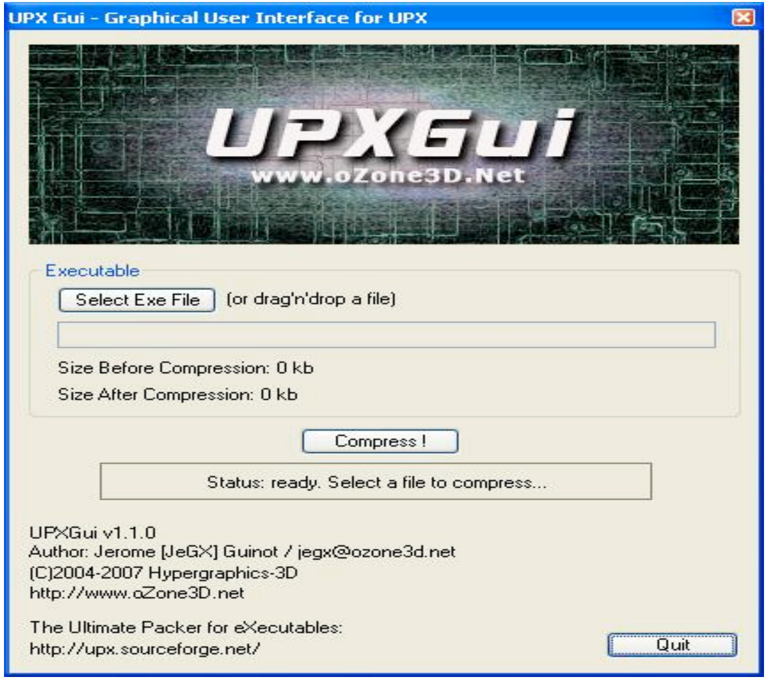
Compress build by **UPX v3.04w**: □

Kill **Zeus**: □

Your system is clean

Christopher C. Elisan

Armoring Tools



(or drag'n'drop a file)

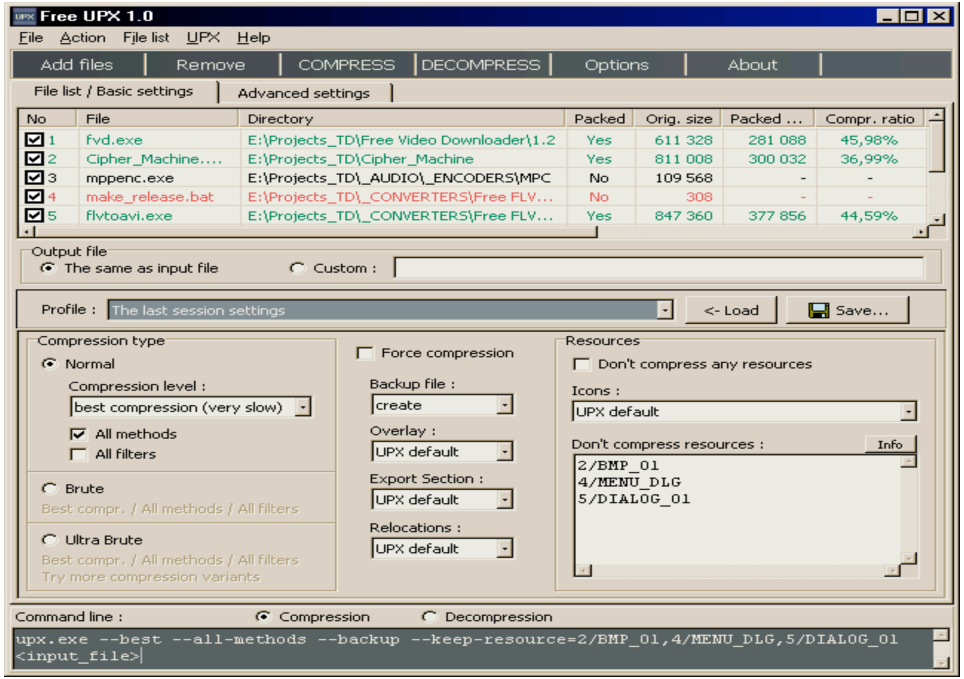
Size Before Compression: 0 kb

Size After Compression: 0 kb

Status: ready. Select a file to compress...

UPXGui v1.1.0
Author: Jerome [JeGX] Guinot / jegx@ozone3d.net
(C)2004-2007 Hypergraphics-3D
http://www.oZone3D.net

The Ultimate Packer for eXecutables:
http://upx.sourceforge.net/



No	File	Directory	Packed	Orig. size	Packed ...	Compr. ratio
☑ 1	fvd.exe	E:\Projects_TD\Free Video Downloader\1.2	Yes	611 328	281 088	45,98%
☑ 2	Cipher_Machine....	E:\Projects_TD\Cipher_Machine	Yes	811 008	300 032	36,99%
☑ 3	mppenc.exe	E:\Projects_TD_AUDIO_ENCODERS\MPC	No	109 568	-	-
☑ 4	make_release.bat	E:\Projects_TD_CONVERTERS\Free FLV...	No	308	-	-
☑ 5	flvtoavi.exe	E:\Projects_TD_CONVERTERS\Free FLV...	Yes	847 360	377 856	44,59%

Output file
● The same as input file ○ Custom :

Profile : The last session settings

Compression type
● Normal
Compression level : best compression (very slow)
☑ All methods
□ All filters
○ Brute
Best compr. / All methods / All filters
○ Ultra Brute
Best compr. / All methods / All filters
Try more compression variants

□ Force compression
Backup file : create
Overlay : UPX default
Export Section : UPX default
Relocations : UPX default

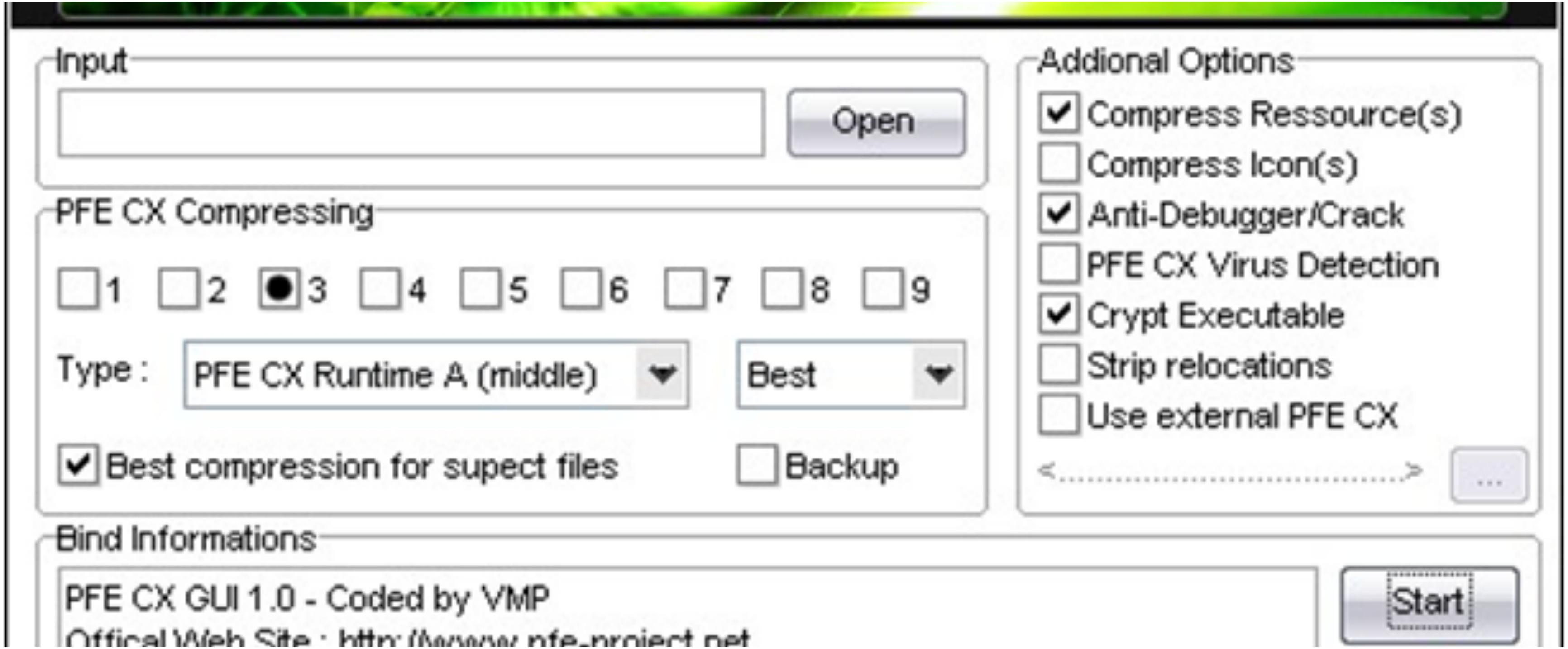
Resources
□ Don't compress any resources
Icons : UPX default
Don't compress resources :
2/BMP_01
4/MENU_DLG
5/DIALOG_01

Command line : ● Compression ○ Decompression

```
upx.exe --best --all-methods --backup --keep-resource=2/BMP_01,4/MENU_DLG,5/DIALOG_01
<input_file>
```

Christopher C. Elisan

Armoring Tools



Input

PFE CX Compressing

□ 1 □ 2 ● 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9

Type : PFE CX Runtime A (middle) | Best

☑ Best compression for supect files

□ Backup

Addional Options

☑ Compress Ressource(s)

□ Compress Icon(s)

☑ Anti-Debugger/Crack

□ PFE CX Virus Detection

☑ Crypt Executable

□ Strip relocations

□ Use external PFE CX

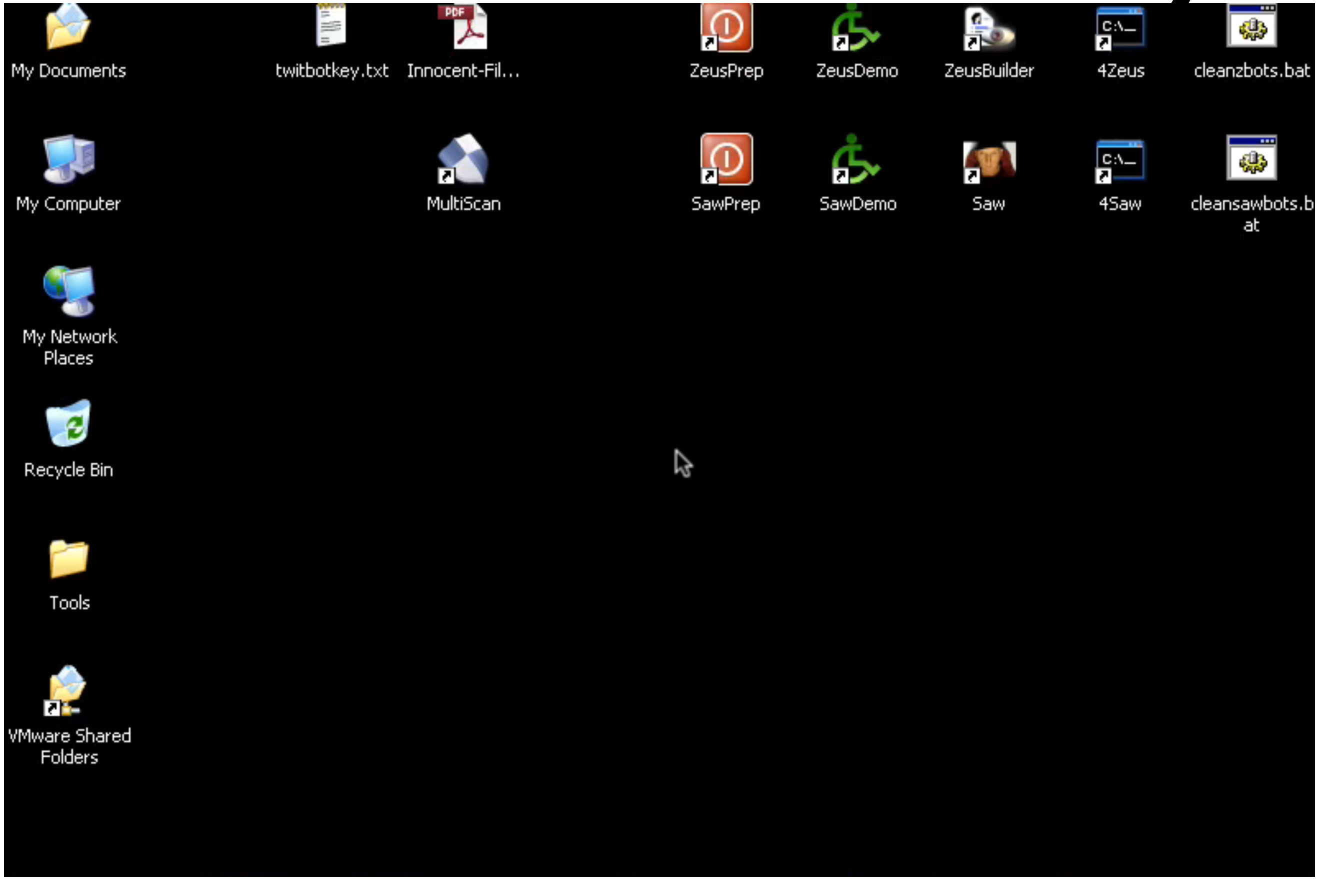
<..................................>

Bind Informations

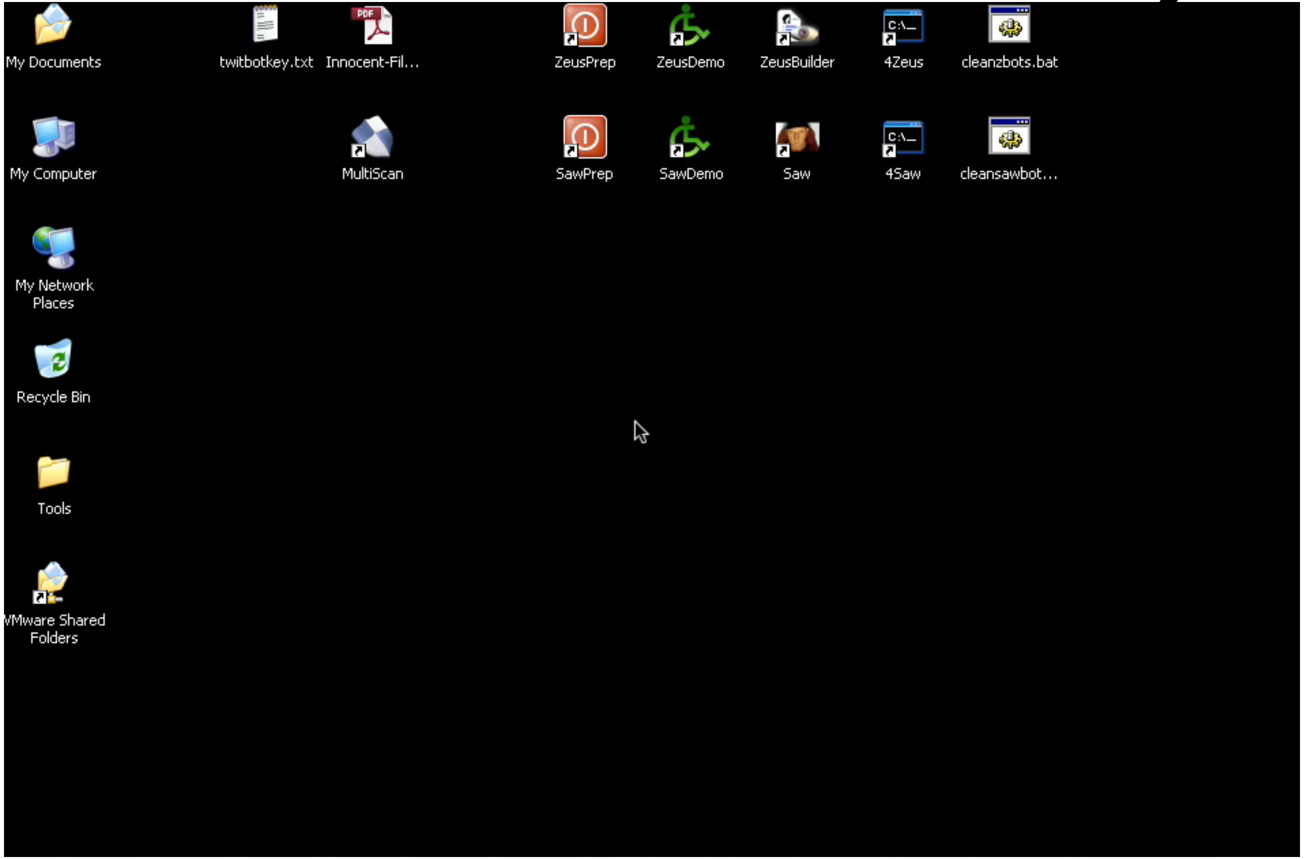
PFE CX GUI 1.0 - Coded by VMP

Offical Web Site : http://www.pfe-project.net

The Malware Factory



The Malware Factory



Lessons Learned

The Whole Picture

- To fully understand the threat, we need to look at the following…
  - Target (Roles, systems)
  - Infrastructure
  - Different roles required to support the infrastructure

Sometimes it is hard, so we collaborate

- Technical
  - Research
  - Scientific approach
  - Knowledge Sharing
- Legal
  - Work with LEOs
  - Share evidence to appropriate entities

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