Malware Automation

Christopher C. Elisan
Principal Malware Scientist
RSA
ABOUT ME

• Principal Malware Scientist
• Past Adventures
  – Damballa (2009-2012)
  – F-Secure (2006-2009)
• @Tophs
• [bit.ly/tophsblog](bit.ly/tophsblog)
ABOUT US

- RSA’s elite, highly trained global threat research and intelligence team
- @RSAFirstWatch
- blogs.rsa.com
PURPOSE OF THE TALK

An over-the-shoulder view of how attackers produce the staggering amount of malware released in-the-wild...
AGENDA

• Current State of Malware
• The Attacker’s Arsenal
• AoAM Creation Process
• Advantages of Automation
• Demo
CURRENT STATE...
LONE WOLF

I DO YOUR BIDDING, MY LORD!
ARMY OF ARMORED MALWARE
IS IT WORSE THAN WE THOUGHT?
THE ATTACKER’S ARSENAL

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

Nowhere Man proudly presents

Virus  Creation  Laboratory

Version 1.00

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

Spy Eye v1.0

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:

[ ]

Make config & get build
Get build

Are you infected by SpyEye?
Your system is clean

Christopher C. Elisan
DIY KITS
ARMORING TOOLS

[Image of a software interface for ARMORING TOOLS, showing options for compression and protection features.]
ARMORING TOOLS
ARMORING TOOLS
AV SCANNERS

![Multi AV Scan 1.6.1 Image]
AV SCANNERS

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.

Select file to scan (20 MB max):

- Do not distribute the sample

QUICKLY DELETE FOLDERS
SECURELY DELETE FILES
THE PROCESS

Quality Assurance

On-premise AV

In-the-Cloud AV

DIY Kit Malware

Old Malware

Copyright Malware, Rootkits and Botnets: A Beginner’s Guide

Christopher C. Elisan
QA DEPENDENT ON ATTACK TYPE
TARGETED ATTACK
OPPORTUNISTIC ATTACK
OPPORTUNISTIC ATTACK
OPPORTUNISTIC ATTACK
ADVANTAGES

• Exponential effect – strength in numbers
• Easy malware update
• Knock AV Out
EXPONENTIAL EFFECT

Malware DiY Kit

Armoring Tool 1

Armoring Tool 2

Christopher C. Elisan
EASY MALWARE UPDATE

• Unique samples per malware deployment technology
• Malware serving domains can rotate malware in minutes
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
STFU

ALREADY
PUTTING THEM TOGETHER

Kit-produced samples

Armored samples

VM with KIT

VM with Armoring Tools

Christopher C. Elisan
KEY TAKEAWAYS

• 1 : MANY
• Commoditization of Skills
• Ask the hard questions from your security provider
• Educate yourself