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

MALWARE, ROOTKITS & BOTNETS
Christopher C. Elisan
2012

Advanced Malware Analysis
Christopher Elisan
2015
Co-Author of

Hacking Exposed
Malware & Rootkits
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**

- **Malware Components**
  - Configuration File
  - Attack Component
  - Regeneration Component
  - Rootkit Component
  - Bot Agent

- **Deployment Technology**
  - Installs Malware Components
  - Deploys the Malware Installer
  - Checks for updates before installation

- **Drop Zones**
  - Drops stolen information

- **Domain Drop Zone**
  - MC sends status / C&C sends commands

- **Command & Control**
  - MC checks for updates / MSD downloads updates

- **Malware Serving Domains**
  - Serves Domains
  - Checks for updates before installation

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

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

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

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

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

- DiY Kits
- Armoring Tools
DiY Kits

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

Spy Eye

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
Armoring Tools

Christopher C. Elisan
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/CCCELISAN
LINKEDIN.COM/IN/ELISAN

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