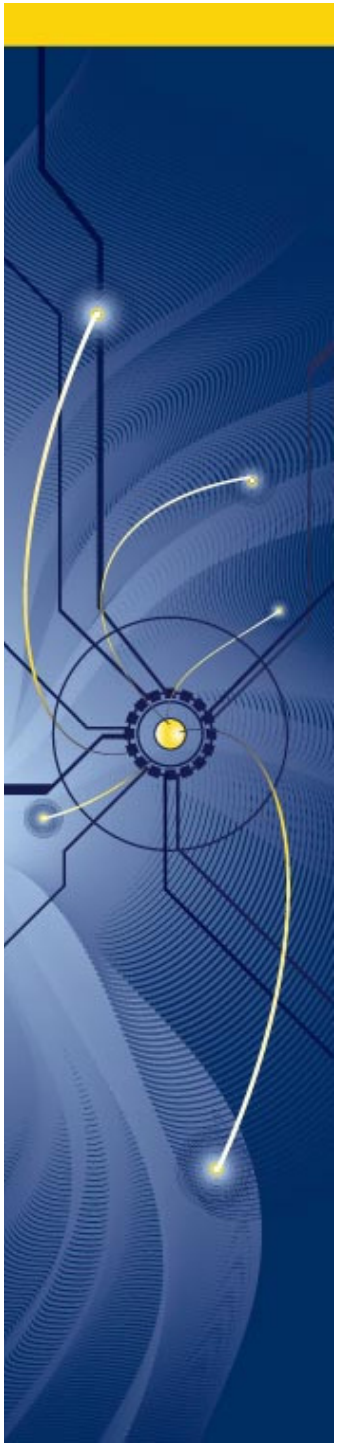


DAMBALLA

Take Back Command-and-Control

I just built what?

Why Badguys do it better…

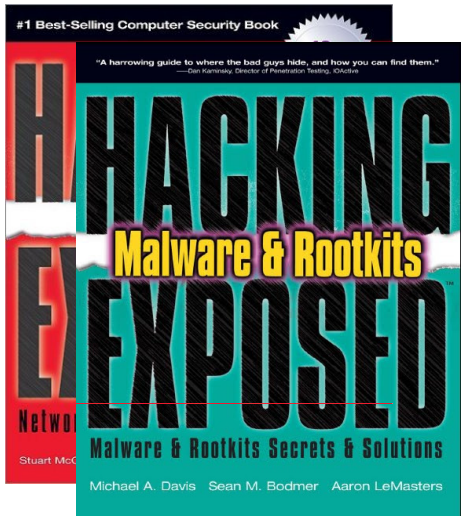
TakeDownCon 2011

Presented by:

Sean Bodmer

Who is this guy?

- Sean M. Bodmer, CISSP, CEH. DODCPT,NSACIA
  - Senior Threat Intelligence Analyst
- Brief Bio
  - Purveyor of unorthodox ideas
  - Interested in learning more about Sith and their economy
  - Over 14 Years in IT Systems Security
    - Attack & Exploitation
    - Intelligence Analysis & Attribution
    - Cyber Counter-Intelligence
  - Over 9 Years in Intelligence and Counter-Intelligence Operations
  - Co-Author: Hacking Exposed Malware & Rootkits 1st Edition
    - ISBN: 0071591184
  - Co-Authoring : Tradecraft: Countering Cyber-Espionage and Advanced Cyber Threats
    - ISBN: 0071772499 (Release Expected Q1 2012)



2011 Q1 Sith Achievements

- **Anonymous**
  - Attacking/Infiltrating numerous enterprises
    - Government
    - Private Sector
- **RSA**
  - Seeds and components of source stolen
- **Energy Firms Pummeled**
  - Targeted by purported State Sponsored Cyber Threats (SSCT)
- **Millions of systems breached**
  - Millions of identities and $$ stolen
- **Spy-Zeus (SpyEye 1.3+)**
  - In late 2010 the source for Zeus Kit was sold to the Roman team
  - In early 2011 Spy-Zeus (SpyEye 1.3) was seen in the wild
    - Largest threat in Q1 to-date

Q12011 Jedi Achievements

- **Coreflood Takedown**
  - > 2m botnet under control of the US DoJ
    - That makes me nervous for other reasons…
- **1 Romanian Hacker Prosecuted**
  - For crimes from 2006 (Shout-Outs to BMW)
- **5 Arrested over WikiLeaks related cyber-attacks**
  - BFD… that didn't even dent the Anon group
- **3 Arrested over SpyEye Assisted Bank Fraud**
  - Another BFD… low level cyber-criminals
- **Am I missing anything??**

Who's keeping score?

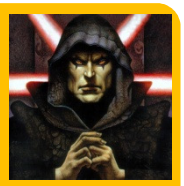
Bad Guys	2011 Score	Good Guys	2011 Score

COFFEE WITH VODKA

no comedy, just caffeine and alcohol.

The Criminal Operations Team

Malware Author(s)

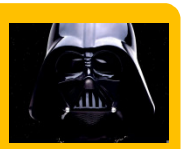


- Original malware creator(s)
- Offer malware "off-the-rack" or custom built
- May offer DIY construction kits
- Money-back guarantee if detected
- 24x7 support

Botnet Master

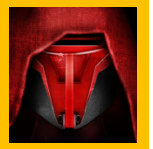
- Individual or criminal team that owns the botnet
- Maintains and controls the botnet
- Holds admin credentials for CnC

Botnet Operator



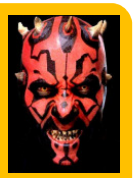
- Operates a section of the botnet for direct financial gain
- Issues commands to the bot agents
- May be the **Botnet** Master

Distribution Provider (MSP)



- Attracts and infects victims
- Specialized distribution network
- 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

Hacking Ecosystem

- Each piece of information, each tool, and every vector has a price

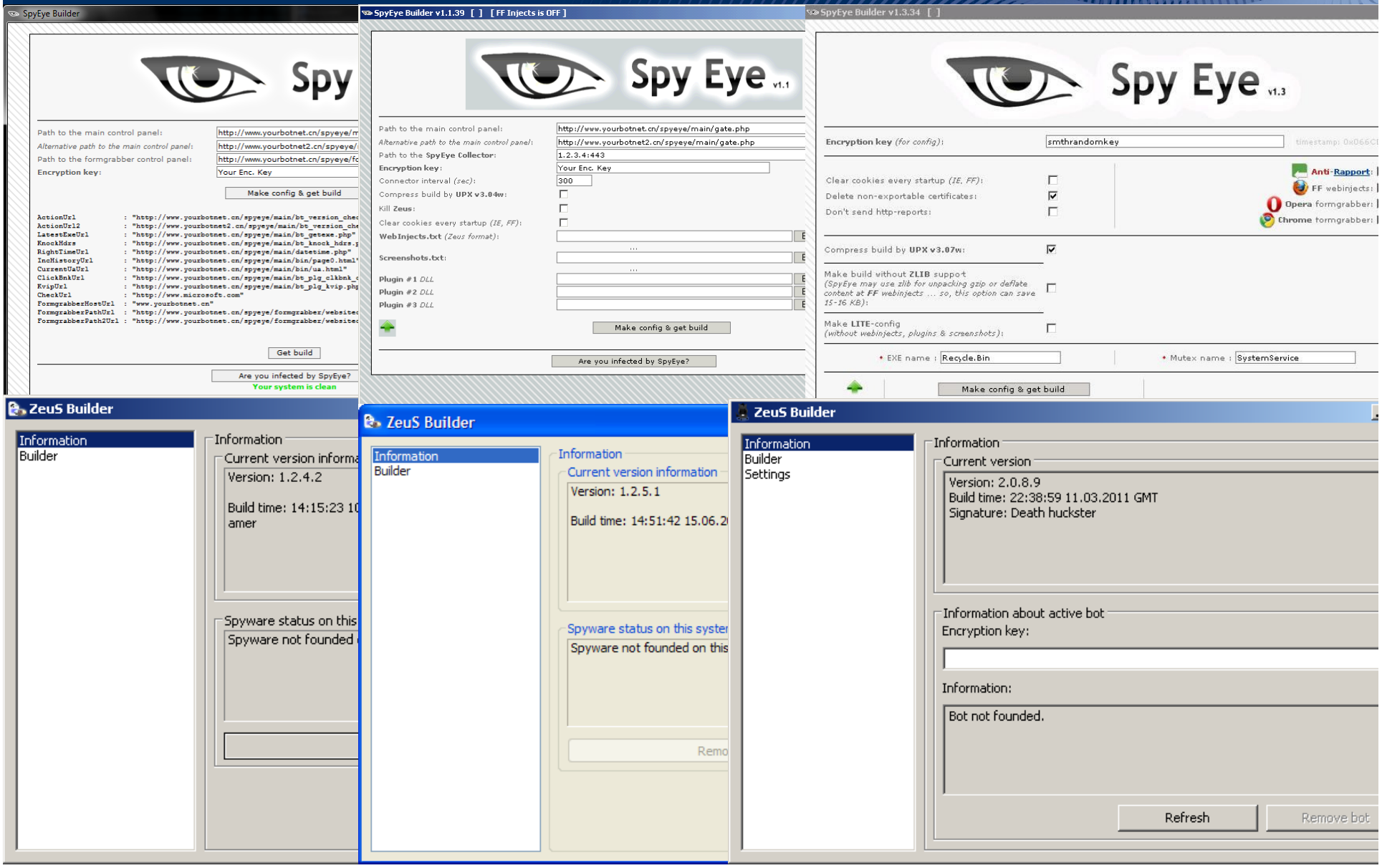
Thank You George Lucas


Rus | Eng
GangstaBucks.com
Statistic
Home
Conditions
Registration
Tariffs
Contacts
GangstaBucks.com - it pays on time!
We pay for all installs!

Moving on Up!


GangstaBucks.com
Statistic
Links
Rates
Setup
Rates:
US 160$
CA 100$
AU 140$
GB 140$
Asia
CN,JP,TW,TH,IN,HK,ID,KP,KR,SG,PH,MY,VN 8$
Europe
AT,BE,CH,DE,DK,ES,FR,GR,IE,IT,MC,NL,NO,PT,SE,NZ 50$
Other 20$
GangstaBucks

Botnet Streamlining



DAMBALLA

Why are you crying?


HOME
BREWING
KIT
PALE ALE
ALL MALT

DAMBALLA

Take Back Command-and-Control

Thank You

Sean Bodmer

email: sbodmer@damballa.com
Web: http://www.damballa.com Blog: http://blog.damballa.com