Low Business Interest in Botnet?

Source: LSEC, Innovations, Websense, 09/13
ACDC
&
The European Commission’s
Cyber Security Strategy

Trust and Security
DG CONNECT - European Commission
1. Economic and social benefits of the Digital Single Market
2. Risks and incidents on the rise > Lack of trust, economic losses, missed opportunities
3. Cross-border nature of risks and incidents
4. Insufficient national preparedness and cooperation across the EU

**EU Cybersecurity Strategy Objective and Priorities**: “To ensure a safe and resilient digital environment in respect of fundamental rights and EU core values”

1. Legislative proposal on Network and Information Security (NIS)
2. Fighting botnets, ensuring the security and resilience of Industrial Control Systems and Smart grids
3. Awareness raising
4. Public-Private Partnerships

**Significance of ACDC for the EC Strategy**

- **First Element of the Strategy to be launched**
- **First test to prove Commissioner Kroes points:**
  - “[cybersecurity] can only happen when all actors play their part and take up their responsibilities.”
  - “Cyber threats are not contained to national borders: nor should cybersecurity be”
- **Conclusion: success of ACDC central to success European cybersecurity policies**
Facts and Figures

- **EC CIP PSP Project**: (CIP-ICT PSP-2012-6 - Obj. 5.1: Cyber security Pilot B)
  - 2012 European Commission Competitiveness and Innovation Program
  - Policy Support Program
  - Pilot Action B: pilot action against botnets

- **Consortium**: 28 partners from 14 Member States
- **Budget**: 15.5 mio € - 50% support by the EC
- **Duration**: 01. FEB 2013 until FEB 2016

What you know: how a botnet works

[Diagram showing the operations of a botnet]

Source: PCWorld
Botnet 1: Centralised

Botnet 2: P2P

Botnet 3: Fast Flux

Botnet 4: Locomotive

Source: ENISA, 2011: Botnets: Detection, Measurement, ...

What you've found out: too many parties

<table>
<thead>
<tr>
<th>Objective 1</th>
<th>Objective 2</th>
<th>Objective 3</th>
<th>Objective 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking down C&amp;C, com. channels, botnet masters</td>
<td>Removing bots from infected computers</td>
<td>Removing malware from web sites</td>
<td>Mitigating the impact of botnets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law enforcement agencies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection Agencies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government regulatory authorities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government cybersecurity experts (e.g. CERFs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISPs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial institutions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managed security service providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web service/Cloud providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web hosting providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus/Firewall/Scanner Vendors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Name Service providers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Name Registrars</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness raising initiatives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Researchers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software &amp; Hardware producers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: ENISA, 2012: DG INFSO CP PSP
28 partners – 14 member countries

ACDC Team

© Leaders in Security – LSEC, 2013, for ACDC – public, p. 11

Consortium Structure

EC Botnet Fighting Team

Pan-European Approach

- extensive sharing of information – without boarders:
  → across networks & member states
- provide a complete set of solutions:
  → accessible online for mitigating on-going attacks
- use the pool of knowledge
  → to create best practices
  → to support affected end customers & organisations in raising their cyber-protection level
- create a European wide network of cyber-defence centres
Solution

Tool Set
From Detection to Protection
Operational Detection

CARNet (KR) have produced a network of detection systems which identify botnet activity within spam e-mails and network connections.

Operational Detection

XLAB have produced an Intrusion Detection System for Android smart phones.
Data Sharing & Analysis

CARNet creates identified threat information in the STIX format and sends the information to the ACDC STIX Aggregator.

The XLAB Android IDS infrastructure queries the STIX Aggregator to obtain threat information provided by CARNet and blocks access to suspicious sites.
Types of Information Currently Collected

- URLs hosting suspected malware
- Malware samples
- IP Addresses of hosts sending SPAM
- IP Addresses of suspected Command and Control Servers
- ...

Collected from Honeypot Networks, SPAM collection systems and Custom partner tools.

Types of Information Currently Collected

<table>
<thead>
<tr>
<th>Source ID</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>52242119579</td>
<td>1,000</td>
</tr>
<tr>
<td>6610661744</td>
<td>1,000</td>
</tr>
<tr>
<td>5232208609</td>
<td>1,000</td>
</tr>
<tr>
<td>1512615864</td>
<td>1,000</td>
</tr>
<tr>
<td>240041923115905</td>
<td>1,000</td>
</tr>
</tbody>
</table>

STIX Document Types Month to date

- Orchestration - Scriptlet
- Observations - Email
**Future Analysis**

Every bot has about 5 Mbps upload bandwidth

- GB: 5.40 Mbps
- APEC: 5.31 Mbps
- EU: 4.32 Mbps
- OECD: 3.53 Mbps

(and about 12 Mbps download bandwidth, too)

Source: IFIS, January 2013

**Other Sensors & Impact**

16,497 Newly Discovered Malware Samples (1 month)

- 66% Undetected by traditional AV vendors
- 80% 13,256 samples generated internet traffic
- 59% Of those samples, 7,918 generated evasive traffic

Source: Palo Alto March 2013
User Tools & Impact

https://www.initiative-s.de/de/index.html
Effective Cyber Threat Intelligence and Information Sharing

http://stix.mitre.org/

Organization & User Impact

Infected machines vs subscribers per ISP (spam)

Source: Botnet mitigation and the role of ISPs, TU Delft, March 2013

Support Centers

© Leaders in Security – LSEC, 2013, for ACDC – public, p 29
But, we need your help!

Why is this one more dangerous than that one?

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Botnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ZeroAccess</td>
</tr>
<tr>
<td>2</td>
<td>Conficker</td>
</tr>
<tr>
<td>3</td>
<td>Dorkbot</td>
</tr>
<tr>
<td>4</td>
<td>Sality</td>
</tr>
<tr>
<td>5</td>
<td>Ramnit</td>
</tr>
<tr>
<td>6</td>
<td>Zeus</td>
</tr>
</tbody>
</table>

Join ACDC

Building Community Portal, Reaching out to:
industry, research, existing communities, law enforcement
policy makers, isp’s & operators, CERTs, ...

Looking for:
1. Detection & Mitigation Tools & Techniques
2. Data Analysis and Botnet Analysis & Prevalence
3. Data & Intelligence Sharing
4. Awareness Creation
5. Influencing Policy
NOT THE END

More information and follow-up

www.acdc-project.eu
www.botfree.eu

Q or C
Ulrich Seldeslachts
ulrich@lsec.be
+32 475 71 3602

• Council conclusions on Critical Information Infrastructure Protection


• Digital Agenda for Europe - COM(2010)245 of 19 May 2010

• The EU Internal Security Strategy in Action: Five steps towards a more secure Europe COM(2010)673

• Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" - COM(2009) 149