FIRST Conference – ISOC – CARIS Workshop
ACDC European Cyber Defence Pilot Experience

Ulrich Seldeslachts, Berlin, June 19th, 2015

Source: Unit42, PA Wildfire, Threat Trend December 2014

Constantly Under Attack

Sources: www.botvrij.be – digitalattackmap.com

Source: GlobalThreatMap Today

Source: Unit42, PA Wildfire, Threat Trend December 2014
Flow

1. Botnet Relevance?

2. SIEM Next Step: Information Sharing

3. ACDC: European Advanced Cyber Defense Center

4. About LSEC
Botnets?

What Botnets do

Source: PCWorld
Botnet 1: Centralised

Botnet 2: P2P

Botnet 3: Fast Flux

Botnet 4: Locomotive

Botnet History


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

Bot Traffic Report 2013
Bot visits are up by 21% to 61.5% of all website traffic

Bot/Human Traffic Distribution
- 61.5% Bot traffic
- 38.5% Human traffic

<table>
<thead>
<tr>
<th>Year</th>
<th>Human (%)</th>
<th>Bot (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>89%</td>
<td>11%</td>
</tr>
<tr>
<td>2013</td>
<td>38.5%</td>
<td>61.5%</td>
</tr>
</tbody>
</table>

Source: RAND, Market for CyberCrime, 2014

Botnets today? DDoS

The Per Hour Cost of a DDoS Attack
- 15% $0 - $4,999
- 17% $5,000 - $19,999
- 26% $20,000 - $59,999
- 17% $60,000 - $99,999
- 15% $100,000 +

Size of Companies Hit by DDoS Attack
- 19% 250-499 employees
- 26% 500-999 employees
- 12% 1,000 - 4,999 employees
- 17% 5,000 - 9,999 employees
- 17% 10,000 or more employees


49% 6-24 hours
8% 1-7 days
4% 7+ days
2% Unsure

~2/3 of attacks last 6+ hours
37% 0-6 hours

Intent of the DDoS Attack
- Flooding your company’s network infrastructure to block all connections to its domain - 33%
- Targeting specific applications to block your company’s use - 40%
- Both - 22%
- Unsure - 5%

Operational Areas Most Financially Impacted by the Attack
- IT group - 35%
- Customer sales - 25%
- Security / Risk management - 12%
- Call center / Customer service - 12%
- Marketing / Public relations - 10%
- Legal - 3%
- Other - 3%


Source: Incapsula, Imperva, 11/2014
Botnets tomorrow : More Sophistication

• Volumetric DDoS Attacks – brute force – with increasing amplification ?
• DNS Infrastructure Attacks? – dns resolver cache flood - taking down nameservers ?
• HTTP attacks – brute force against webservers ?
• Malicious Payloads – exploit server vulnerabilities – ShellShock

• Weaponize Attacks
• AWS Botnet ?
• New Large Botnets

Botnet is Big Business : Example RBN

An Example = Russian Business Network (RBN)

• AS40989 is RBN-AS
• Malware – Gozi, Torpig,…..
• Toolkits – Mpack…, attack tools
• Botnets – fast flux
• Fake Anti-virus
• Cybercrime as a service - 76Service…. Loads….iFrame
• Child pornography hosting
• Cybercrime affiliate payment systems
• Cyberwar – Georgia
• AbdAllah Franchise (2014)
• 2007 – Est. gross revenue $1.2 billion – Net $200 million

Source : Cyberdefcton 03/2014 at LSEC, Infosecurity
Using webservices, Botnet as a Service, ...

Source: McAfee, Cybercrime Exposed, October 2013

Doesn’t impact your business?

Source: IBM, X-Force Trends Report 09/2013
Attribution: top causes of data breaches 2012 - 13

But who cares? – Business? – not really

Source: ISTR, October 2013, www.lsec.be


Source: LSEC, Innovations, Websense, 09/13

Should we even care?

Carna Botnet: 420,000 bots – a research project

60k virus on an infected device:
- Open a port for remote access by the central internet mapping systems.
- Reach out to scan and record details about a subset of the rest of the internet.
- Identify routers with telnet open onto the internet and a weak root password, e.g. root:root, admin:admin or either account with no password.
- Login and install the virus on the next open router in the ever-growing tree of zombies.
- For research purposes!
The point?

Global Threat Map Today

Source: Hostexploit, March 2014
Botnet Relevance for Business

Godzilla Through the Years

Why Information Sharing?
Business Case components for trusted sharing
Forrester defines threat intelligence as:

Source: Forrester Research, 2014

- Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.
- We share at about the same speed that George R.R. Martin writes novels, which is slow
- Quid pro quo and relationship driven
- You cannot automate trust

**Circle of trust**

Not alone ... need to differentiate
The need for Active Defense

WHY ARE WE WAITING FOR THE ATTACK TO HAPPEN?

Source: RSA Conference, OpenDNS, 02/14


The Threat landscape

Web-based malicious activity has accelerated
- Primary vector for malicious activity
- Target reputable, high-traffic websites

Cyber criminals want YOUR information
- Focus on exploits targeting end-users for financial gain

Increased sophistication of the Underground Economy
- Well-established infrastructure for monetizing stolen information

Rapid adaptation to security measures
- Relocating operations to new geographic areas
- Evade traditional security protection

Source: Symantec, DeepSight EWS, 2012

Threat landscape

The Challenge

- How do I gain awareness of the global threat landscape?
- How do I identify threats that could impact my company?
  - 31,850 new malicious code threats per week *
- How do I identify vulnerabilities important to my company?
  - 105 new vulnerabilities per week *
- How do I prioritize my response to vulnerabilities and global threats?
- How do I translate the global landscape to my enterprise?

Source: Symantec, DeepSight EWS, 2012

The Methodology: 1 Collect and Store Security Data

- Traditional Security Operations and Technology
  - Logs, Events, Alerts
  - Configuration information
  - System audit trails
  - Identity context
  - Network flows and anomalies
  - Malware information
  - External threat feeds
  - People
  - Data
  - Applications
  - Infrastructure

Monitor Everything

Source: LSEC Big Data, IBM 0/14

The Methodology: 2 Real-time and historical analysis

- Descriptive Analytics
  - What happened?
  - How many, how often, where?
  - What exactly is the problem?
  - What is the impact?
- Historic and Predictive Analytics
  - Has it happened before?
  - What if these trends continue?
  - What might happen next?
- Decision modeling
  - What actions can we take?
  - How can we avoid this in future?
  - How can we mitigate risk?

Data → Information → Security Intelligence

Source: LSEC Big Data, IBM 0/14


Operations Incident Handling

In reality, 25 hour incident ... and 11 hours before the effect

Source: LSEC Hardening, CrossRoad 03/14


Operations Incident Handling: reducing attacker free time


Big Data in Security Events

Source: RSA Conference, Intel 03/14


Analysis of incidents and threats

Source: RSA Conference, Intel 03/14

Breach Notification – required / voluntary

Hack victims urged to share the gory details

Advanced Cyber Security Center fosters voluntary information sharing among private organizations via a way of staying ahead of the bad guys


Press release

Government launches information sharing partnership on cyber security

New cyber partnership launched to help government and industry share information and intelligence on cyber security threats.


Example Regulatory : Telecom

Those looking to multiply their knowledge, should be prepared to share some first

Example Voluntary – Information Sharing

EDA Project Team Cyber Defence

Start: Nov 2011

Ann.: Within the remit of the Cyber Security Strategy for the EU to answer short-, medium- and long-term Cyber Security capability requirements and to identity collaborative options in order to improve Cyber resilience of PdIS and ISCF operators.

Parties: EDA (led), NL, DE, PT, BE, RO, SI, SE, UK, FR, IT, LV, GR, HU, EL, EL, PT, FR, HU, LT, LV, NL, PL, PT, RO, RE, BE, UK, FR, IT, NO on a regular basis plus EUMM Council (OS), EUMM, EDA, EIS, EU (led)
Example Voluntary – Information Sharing

Multinational Alliance for Collaborative Cyber Situational Awareness

Information Sharing: NISP Survey Results

<table>
<thead>
<tr>
<th>Distribution 1</th>
<th>Distribution 2</th>
<th>Distribution 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>National (71%)</td>
<td>Regional Multi (29%)</td>
<td>International (13 schemes)</td>
</tr>
<tr>
<td>Single Sector (9%)</td>
<td>Cross Sector (25%)</td>
<td></td>
</tr>
<tr>
<td>Mandatory Participation (47%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free to Access Scheme (80%)</td>
<td>Subscription Required Access Scheme (14%)</td>
<td>Both (If the subscribing services use a subset of services use free based on specific criteria) 3 schemes</td>
</tr>
<tr>
<td>Information Sharing Schemes (27)</td>
<td>Pure Incident Notification Schemes (1)</td>
<td>Providing for both Incident Notification and Information Sharing (27)</td>
</tr>
<tr>
<td>Formal Sharing Protocol incorporated (44%)</td>
<td>Internal Sharing/Notification Protocol incorporated (41%)</td>
<td></td>
</tr>
<tr>
<td>&gt;20 Participating Organisations (14%)</td>
<td>&gt;20 x4M Participating Organisations (18%)</td>
<td>&gt;40 Participating Organisations (29%)</td>
</tr>
<tr>
<td>Email Communications Supported (34%)</td>
<td>Portal Sharing Platform (25%)</td>
<td>Support for Automated exchange of information &amp; indicators (35%)</td>
</tr>
<tr>
<td>Scheme Operating &gt; 5 years &lt; 10 years (14)</td>
<td>Scheme Operating &gt; 5 years (14)</td>
<td>Scheme Operating &gt; 5 years (14)</td>
</tr>
<tr>
<td>Schema has Bio Physical Community Meetings (1)</td>
<td>Scheme has Community Meetings between 3-2 time per year (1)</td>
<td>Scheme has Community Meetings more than 2 time per year (1)</td>
</tr>
</tbody>
</table>
| Website in place for Scheme (30%) | No Website In place | }
Howto: Incident Management Tools

STIX™ Effective Cyber Threat Intelligence and Information Sharing

Information Sharing: commonalities, no conflict

Consider these questions:

- What activity are we seeing?
- What threats should I look for on my networks and systems and why?
- Where has this threat been seen?
- What does it do?
- What weaknesses does this threat exploit?
- Why does it do this?
- Who is responsible for this threat?
- What can I do about it?

http://stix.mitre.org/
Fragmented response

<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 and services</td>
<td>Mitigating the impact of botnets</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. CERTs)</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 CIP PSP

28 partners – 14 countries

ACDC Team

Prufboerger FNKE
G Data Software AG
Institut für Informatik und Angewandte Mathematik, Universität des Saarlandes
INTEGeo – National Institute of Geomatics
KU Leuven
LSEC - Leaders in Security
Microsoft EMEA
SignaturIT
Telecomitalia
Telefónica I+D
University of Technology, Dortmund
XLAB – Plaça de les Ciències, Universitat Politècnica de València
Fundació Privada Barcelona Digital Centre Tecnologic
Istituto Superiore Dalle Comunicazioni e delle Technologie dell’Informazione
Montimage
AC up to today – DC

1. Achievement Highlights
   1. Collaboration 28 partners, 14 countries, +40 external partners
   2. Sensors operational, sensing, analyzing, reporting locally & sending data to Central Clearing House (CCH)
   3. New sensors installed & operational (eg Darknet)
   4. CCH operational and collecting and transmitting data (JSON, YAML), STIX integration
   5. Decentralized Data Analysis with 6 different industrial partners
   6. Reporting into CERTs, ISP’s, LEA’s ... end users
   7. Setup of 11 National Support Centers
   8. Different resulting tools : Mobile, Ransomware, Website Check, ...

2. Challenges Highlights
   1. Regulatory Framework : Data Protection vs Monitoring
      1. Consent
      2. Controlled :
         1. ISPs – CERTs by exception
         2. Industry – delegated
   2. Performance & Capability of Detection & Takedown
   3. Sustainability of the Community : sign up today!
Data Sharing: Example & Effect

CARNet creates identified threat information and sends the information to ACDC.

The XLAB Android IDS infrastructure queries the CCH to obtain threat information provided by CARNet and blocks access to suspicious sites.

XLAB Mobile IDS: Device Monitor

- 33 Android botnets
- 1 co Symbian botnet with the same C&C
- 2 Symbian botnets
- 3 Blackberry botnets

Statistics from 10/8/2014, 14.077 infections total

Source: K&A Virus Tracker, Botconf 2014
Available on Google Play Store

- Demo videos: [http://x.k00.fr/zmprk](http://x.k00.fr/zmprk)

Tools in Production to Solutions

ATOS AHPS, commercial SIEM

Tools in Production to Solutions

ATOS Netflow Behavioral Analysis

Darknet Subpilot

A Darknet is a portion of routed, allocated IP space in which no active services or servers reside. These are "dark" because there is, seemingly, nothing within these networks.

A Darknet does in fact include at least one server, designed as a packet vacuum. This server gathers the packets and flows that enter the Darknet, useful for real-time analysis or post-event network forensics.

Any packet that enters a Darknet is by its presence aberrant. No legitimate packets should be sent to a Darknet. Such packets may have arrived by mistake or misconfiguration, but the majority of such packets are sent by malware and BOTNETS!
Darknet Subpilot

- Darknet Results: Most Seen ASN's

<table>
<thead>
<tr>
<th>ASN</th>
<th>Name</th>
<th>Country</th>
<th>Subnet sizes</th>
<th>Requests</th>
<th>Request ratio</th>
<th>HE Rank</th>
<th>HE Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>16276</td>
<td>OVH</td>
<td>FR</td>
<td>1,090,816</td>
<td>124,059</td>
<td>0.114</td>
<td>12</td>
<td>182.24</td>
</tr>
<tr>
<td>4134</td>
<td>CHINANET</td>
<td>CN</td>
<td>104,621,312</td>
<td>55,003</td>
<td>0.001</td>
<td>46</td>
<td>124.88</td>
</tr>
<tr>
<td>6939</td>
<td>HURRICANE</td>
<td>US</td>
<td>260,864</td>
<td>37,095</td>
<td>0.142</td>
<td>393</td>
<td>60.49</td>
</tr>
<tr>
<td>29073</td>
<td>EGATEL</td>
<td>NL</td>
<td>9,984</td>
<td>31,850</td>
<td>3.190</td>
<td>19</td>
<td>162.89</td>
</tr>
<tr>
<td>34352</td>
<td>COLDCROSSING</td>
<td>US</td>
<td>122,368</td>
<td>25,899</td>
<td>0.212</td>
<td>229</td>
<td>74.32</td>
</tr>
<tr>
<td>12876</td>
<td>ONLINE S.A.S.</td>
<td>FR</td>
<td>180,224</td>
<td>24,290</td>
<td>0.135</td>
<td>1,371</td>
<td>29.02</td>
</tr>
<tr>
<td>4837</td>
<td>CHINA169</td>
<td>CN</td>
<td>53,008,896</td>
<td>23,811</td>
<td>0.000</td>
<td>48</td>
<td>122.68</td>
</tr>
<tr>
<td>3462</td>
<td>HINET</td>
<td>TW</td>
<td>8,085,504</td>
<td>13,983</td>
<td>0.002</td>
<td>123</td>
<td>92.50</td>
</tr>
<tr>
<td>45090</td>
<td>CNNIC-TENCENT</td>
<td>CN</td>
<td>6,656</td>
<td>13,873</td>
<td>2.084</td>
<td>45,553</td>
<td>0.19</td>
</tr>
<tr>
<td>4766</td>
<td>KIXS-AS</td>
<td>KR</td>
<td>29,005,312</td>
<td>12,895</td>
<td>0.000</td>
<td>262</td>
<td>70.58</td>
</tr>
</tbody>
</table>

- Providing Input into: Hostexploits Report on Zeus Botnet

Source: [http://hostexploit.com](http://hostexploit.com), March 2014

User Tools & impact

http://www.check-and-secure.com
User Tools & Impact

https://www.initiative-s.de/de/index.html

Herzlich willkommen beim Seiten-Check der Initiative-S!


ACDC Online 1: End User

www.botfree.eu

Connecting **users** to **solutions** through a set of European support centres

ACDC Online 2: Project

www.acdc-project.eu

Operating as a European pilot project
ACDC Online 3 : Community

- Operating as a community
- Joining forces to fight botnets
- Sharing intelligence
- Learning from tools & technologies and effects
- Expert network

https://communityportal.acdc-project.eu
ACDC Online 3: Community

About LSEC
About LSEC & the Belgian R2GS Chapter

You’re welcome to join us to become a leader in security

Ulrich Seldeslachts, Paris, December 17th, 2014
About LSEC Summary

1. Leaders In Security: a non-profit Flemish (vzw) industry association and user community supporting innovation & development of information security
   1. Data protection: protection of data, users, information and systems,
   2. Security management: standards, legal, good practices
   3. Tools and technologies: networking, encryption, virtualization
2. Over 135 members, e-security companies, reaching out to more than 25,000 ICT professionals and security professionals, operations in Be, Ni, UK
3. Strategic partners in ICT, TMT, Industry, Finance, Healthcare, Energy, ... and in Germany, UK, Spain, France, Italy, Czech Republic, Ireland, US, ...
4. Various international projects
   1. FIRE
   2. ACDC
   3. NEBUCOM
   4. IPACSO
   5. ...
5. More than 100 activities per year in Belgium and abroad:
   1. Seminars, Conferences, trade shows, ...
   2. www.lsec.be with over 5000 documents (white papers, business cases, presentations, ... on information security related matters)
   3. Regular newsletters, invitations, discussion for a
   Visit www.lsec.be for more information and documentation

NOT THE END

More information and follow-up

www.lsec.be
www.leadersinsecurity.org

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